

SMR Linux Series
Smart Megapixel Video Recorder
User Manual

Release 1.2



About This Document

This manual introduces the hardware components of THE SYSTEM series and describes how to install them. It also provides an overview of Server surveillance functionality, and includes the functions of Video Management Software for operating and monitoring a Server network.

Version History

Version	Description	Date
1.0	Initial release	May 2015
1.1	UI Updated	May 2015
1.2	New models added	Aug. 2015

Copyright Statement

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written consent of Surveon Technology Inc.

Disclaimer

Surveon Technology makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Surveon Technology reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation to notify any person of such revisions or changes. Product specifications are also subject to change without notice.

Trademarks

Surveon and Surveon logo are trademarks of Surveon Technology Inc. Other names prefixed with “NVR” and “SMR” are trademarks of Surveon Technology Inc.

- Microsoft Windows and Windows are registered trademarks of Microsoft Corporation.
- Linux is a trademark of Linux Torvalds.
- Solaris and Java are trademarks of Sun Microsystems, Inc.

All other names, brands, products or services are trademarks or registered trademarks of their respective owners.

Table of Contents

About This Document	2
Version History	2
Copyright Statement	3
Table of Contents	4
Safety Precautions	15
Device Site Recommendations.....	15
Chapter 1. Product Overview.....	16
1.1. Features and Benefits	16
1.2. Specifications for the Linux SMR Series.....	17
1.2.1. Hardware Specifications	17
1.2.2. VMS Specifications	19
Chapter 2. Hardware Overview	21
2.1 Front Panel	21
2.2. Rear Panel	22
2.3. Hard Drive Designation.....	23
2.4. LED Definitions	25
2.4.1. Desktop System Front Panel LEDs for SMR2100, SMR8300.....	25
2.4.2. Desktop System Front Panel LEDs for SMR2110, SMR5110.....	26
2.4.3. Rear Panel Ethernet LED	27
Chapter 3. Software Overview	29
3.1. Software Introduction	29
3.2. Module Framework	30
3.3. System Architecture	32
3.3.1. Standalone Server (Client-Server All-in-One)	33
3.3.2. Standalone Server + Remote Client (Web Client / SPhone Client).....	34
3.3.3. Multiple Servers + SCC Client.....	36
3.3.4. Network Requirements	39
Opening Ports	39
Warnings / Precautions.....	39

3.4. Port Forwarding	40
3.4.1. Port Forwarding for Accessing VMS Server	41
Chapter 4. Installation	44
4.1. Before You Start.....	44
4.1.1. Checklist for Operating Environment.....	44
4.1.2. Checklist for Network Topology.....	44
4.2. Hard Drive Installation	45
4.2.1. Hard Drive Installation Prerequisites	45
4.2.2. Inserting Hard Drive into Drive Tray (Desktop Series)	45
4.3. System Connections	47
4.4. Powering up SMR	49
4.4.1. SMR Systems	49
4.5. Logging into SMR Series	50
4.6. Run the Install Wizard.....	51
Chapter 5. Basic System Settings	64
5.1. Storage Management	64
5.2. Adding Cameras to the Server	66
5.2.1. Automatic Scan for Cameras	66
5.2.2. Manually Adding Cameras.....	68
5.3. Setting Recording Schedule	70
5.3.1. Recording Schedule	70
5.4. Setting up Live View.....	72
Chapter 6 Live View	73
6.1. Live View Window Overview.....	73
6.2. View Setup	76
6.2.1. Switching Between Different Screen Divisions.....	76
Creating and Using New Screen Divisions.....	76
Auto-flipping Pages	76
Screen Division Page Use.....	76
Fisheye View	77
E-map	78

Secondary Display	80
6.3. Functionality Within Views.....	81
6.3.1. Digital Zoom	81
6.3.2. Instant Playback.....	82
6.3.3. Manual Recording	84
6.3.4. Others.....	85
Image Settings	85
Insert.....	86
Send to Large Channel.....	87
Reconnect	87
Remove the Camera	87
6.4. Full Screen View	88
6.4.1. Entering Full Screen View.....	88
6.4.2. Exiting Full Screen Mode	88
Chapter 7. Server Setup	89
7.1. Server Settings.....	89
7.1.1. General Server Settings	89
7.1.2. To perform Notification Setting.....	92
7.1.3. Scheduling Recording	95
7.1.4. Storage Management	97
7.1.5. Pre/Post Recording	99
Chapter 8. Camera Setup.....	100
8.1. Adding Cameras	100
8.1.1. Automatic Scan for Cameras	100
8.1.2. Manually Adding Cameras.....	103
8.2. Camera General Settings.....	105
8.2.1. General Camera Settings.....	105
8.2.2. Edit Camera.....	108
8.2.3. OSD Settings	110
8.2.4. Privacy Mask Settings.....	112
8.3. Camera Image and Quality Settings.....	114

8.3.1. Camera Image Settings	114
8.3.2. Advanced Video Settings	117
8.4. VI Setup	120
8.4.1. Camera Motion Detection	121
Configuring and Editing Detection Windows.....	122
Deleting a Detection Window	122
8.4.2. General Motion Detection.....	123
Enabling or Disabling a Detection.....	123
Configuring and Editing Detection Windows.....	123
Testing Detection Windows	124
Deleting a Detection Window	124
8.4.3. Tampering Detection	125
Enabling or Disabling a Detection.....	125
Configuring Tampering Detection.....	125
Testing Tampering Detection.....	126
8.4.4. Forbidden Area Detection.....	127
Enabling or Disabling a Detection.....	127
Configuring and Editing Detection Windows.....	127
Testing Detection Windows	128
Deleting a Detection Window	128
8.4.5 Intrusion Detection	129
Enabling or Disabling a Detection.....	129
Configuring and Editing Detection Windows.....	129
Testing Detection Windows	130
Deleting a Detection Window	130
8.4.6. Virtual Fence	131
Enabling or Disabling a Detection.....	131
Configuring and Editing Detection Windows.....	131
Testing Detection Windows	132
Deleting a Detection Window	133
8.4.7. Missing Object Detection.....	134

Enabling or Disabling a Detection.....	134
Configuring and Editing Detection Windows.....	134
Testing Detection Windows	135
Deleting a Detection Window	135
8.4.8. Foreign Object Detection	136
Enabling or Disabling a Detection.....	136
Configuring and Editing Detection Windows.....	136
Testing Detection Windows	137
Deleting a Detection Window	137
8.4.9. Tailgating Detection	138
Configuring and Editing Detection Windows.....	138
Testing Detection Windows	139
Deleting a Dividing Line	139
Enabling or Disabling a Detection.....	139
8.4.10. Go In/Out Detection	140
Configuring and Editing Detection Windows.....	140
Testing Detection Windows	141
Deleting a Detection Window	141
Enabling or Disabling a Detection.....	141
8.4.11. General Settings.....	142
8.5. PTZ Setup	143
8.5.1. PTZ Setup	143
8.5.2. PTZ Preset Settings	146
Adding a Preset.....	148
Deleting a Preset	148
8.5.3. PTZ Patrol Settings.....	149
8.5. PTZ Controls.....	152
8.5.1. Directional Pad	152
Pan and Tilt	152
8.5.2. Functional Buttons	153
Home	153

Preset	153
Auto Pan	153
Patrol	153
Zoom	153
Focus	153
8.5.3. Deleting a Camera	154
Chapter 9. Alarms and Events	157
9.1. Alarm Rules.....	157
9.1.1. Adding an Alarm Rule.....	158
Conditions	159
Actions	161
Alarm Scheduling.....	166
9.2. Event Log	168
9.2.1. Exporting a Log	169
9.2.2. Searching the Event Log.....	169
System	170
Event Type	170
Operation.....	170
Module Name	170
Device Name	171
User Name.....	171
Performing a Search	171
9.2.3. System Alarm View.....	172
Chapter 10 Search and Playback.....	173
10.1. Introduction	173
10.2. Time Search	174
10.2.1. Time Selection	174
Specified Time.....	174
10.2.2. Use of Various Views Selection	175
10.2.3. Camera Selection	175
10.2.4. Timeline.....	176

10.2.5. Playback	176
Capturing Screenshot	178
Capturing Video Clip	178
10.3. VI Search	180
10.3.1. Creating a VI Search.....	180
Time Selection.....	180
Camera Selection.....	181
Setting New Search Criteria	182
10.3.2. Using the Search Results.....	183
Selecting the Result.....	183
Result Playback.....	183
10.4. Event Search.....	186
10.4.1. Creating an Event Search.....	186
Time Selection.....	186
Camera Selection.....	187
Setting Event Search Criteria	188
10.4.2. Using the Search Results.....	189
Selecting the Result.....	189
Result Playback.....	190
Chapter 11. VMS Setup.....	192
11.1. Camera	192
11.1.1. Edit Camera	192
11.1.2. Advanced Camera.....	192
11.1.3. General Camera Settings	193
11.1.4. Image Settings.....	193
11.1.5. PTZ Camera Settings	193
11.1.6. PTZ Preset Settings.....	193
11.1.7. PTZ Patrol Settings	193
11.1.8. OSD Settings	193
11.1.9. Mask Settings	193
11.1.10. Optimize Settings	194

11.2. VI.....	195
11.2.1. Camera Motion Detection	195
11.2.2. General Motion Detection	195
11.2.3. Tampering Detection.....	196
11.2.4. Forbidden Area Detection	196
11.2.5. Intrusion Detection	196
11.2.6. Virtual Fence Detection	196
11.2.7. Missing Object Detection	196
11.2.8. Foreign Object Detection.....	196
11.2.9. Tailgating Detection.....	197
11.2.10. Go In/Out Detection	197
11.2.11. General Setting	197
11.3. Recording	198
11.3.1. Schedule	198
11.3.2. Storage	198
11.3.3. Pre/Post Recording	198
11.4. Alarm.....	199
11.4.1. Alarm Rules.....	199
11.4.2. Email	199
11.4.3. SMS.....	199
11.4.4. Digital I/O Settings	200
11.5. Account.....	201
11.5.1. Accounts	202
Add Account To add an account to the domain:.....	202
Editing an Account	204
Changing an Account Password.....	205
Deleting an Account	205
11.5.2. Account Authority Settings	206
11.6. Network	207
11.6.1. NVR Settings	207
11.6.2. Web Server	208

11.6.3. Multiple LAN	209
11.6.4. DHCP Settings	210
11.6.5. DDNS Setting	211
11.6.6. Port Mapping	211
11.7. System	213
11.7.1. General.....	213
11.7.2. Advanced.....	213
11.7.3. Display Resolution Settings.....	214
11.7.4. Language	214
11.7.5. Map Editor	215
11.7.6. Log Viewer	215
11.7.7. Optimize Settings	215
11.8. Maintenance	216
11.8.1. Stream Status	216
11.8.2. Upgrade	217
11.8.3. Import/Export	217
Importing Parameters	218
Exporting Parameters.....	218
11.8.4. License	219
11.8.5. System Backup	220
11.8.6. Clear SCC Data	220
11.8.7. Remote Assistant	221
Chapter 12. Remote Web Client and SPhone Client for Simple Use (Optional)	222
12.1. Software Installation for Remote Control	223
12.1. Installing the VMS	223
12.2. Starting the VMS Client	227
12.3. Starting the Web Client.....	229
12.3.1. Checking the Software Version	229
12.3.2. Use of 1x/4x views	229
12.3.3. PTZ Control	230
12.3.4. Playback Settings	231

12.4. Installing and Starting the SPhone Client on iOS Devices	232
12.4.1. Installing the SPhone Client (Optional)	232
12.4.2. Starting the SPhone Client	232
12.4.3. Checking the Software Version	233
12.4.4. Functionalities on the SPhone Client	233
Live View	233
Icon Descriptions	235
Playback	236
PTZ/Preset	236
DI/DO	237
Info	237
12.5. Installing and Starting the SPhone Client on Android Devices	238
12.5.1. Installing the SPhone Client (Optional)	238
12.5.2. Starting the SPhone Client	238
12.5.3. Checking the Software Version	239
12.5.4. Functionalities on the SPhone Client	240
Live View	240
Icon Descriptions	242
Playback	243
PTZ/Preset	243
DI/DO	244
Info	244
Chapter 13. SurveOne (Optional)	246
13.1. Installation	246
13.2. Login	254
13.3. Overview	255
13.4. Monitor	261
Device	261
Network	262
Storage	262
13.5. Workflow	264

Enable Web Server / DDNS.....	264
Back Up Configuration	267
NVR Multiple IP Setup	268
Copy Configuration to Multiple Cameras.....	269
Backup Configuration	270
13.6. Event Log.....	272
Search.....	272
Export.....	273

Safety Precautions



Electric Shock Warning

This equipment may cause electric shocks if not handled properly.

- Access to this equipment should only be granted to trained operators and maintenance personnel who have been instructed of, and fully understand the possible hazardous conditions and the consequences of accessing non-field-serviceable units such as the power supplies.
- The system must be unplugged before moving, or in the event that it becomes damaged.



Reliable Grounding

Particular attention should be given to prepare reliable grounding for the power supply connection. It is suggested to use a direct connection to the branch circuit. Check for proper grounding before powering on the device.



Overloading Protection

The device should be installed according to specifications. Provide a suitable power source with electrical overload protection. Do not overload the AC supply branch circuit that provides power to the device.



ESD Precautions

Please observe all conventional anti-ESD methods while handling the device. The use of a grounded wrist strap and an anti-static work pad are recommended. Avoid dust and debris in your work area.

Device Site Recommendations

The device should be installed according to specifications. This device should be operated at a site that is:

- Clean, dry, and free of excessive airborne particles.
- Well-ventilated and away from heat sources such as direct sunlight and radiators.
- Clear of vibration or physical shock.
- Away from strong electromagnetic fields produced by other devices.
- Available with properly grounded wall outlet for power. In regions where power sources are unstable, apply surge suppression.
- Available with sufficient space behind the device for cabling.

Chapter 1. Product Overview

1.1. Features and Benefits

The SMR series is a state-of-the-art network video recorder features RAID, low power. With bay hard disk trays, the system series is the best in class SMR that supports megapixel quality video of 4 to 64 channels for video retention periods from 7 to 40 days or more. In addition, the system series is fully burn-in-tested and uses preloaded Enterprise VMS to eliminate compatibility issues while reducing maintenance overheads. It is out of question that the system series is the most reliable and cost-effective solution for small to medium sized surveillance needs.

1.2. Specifications for the Linux SMR Series

1.2.1. Hardware Specifications

	SMR2100	SMR2110	SMR5110
System Processor	Intel Dual Core	Intel®Celeron Dual Core 2.0 GHz	Intel®Celeron Dual Core 2.0 GHz
System Memory	DDR3 2GB	DDR3L 4GB x1	DDR3L 4GB x1
Operating System	Linux Embedded System		
Storage	3.5" SATA HDDs x2		
	HDD hot swappable with LED status indicator		
I/O Interface	RJ-45: 2x Gigabit Ethernet USB: 4x USB2.0 VGA(D-Sub): x1, E-STAT: x1	RJ-45: x1 Gigabit Ethernet USB: USB 3.0 x1, USB 2.0 x3 VGA: DVI-I x1 Serial: x1 (support RS232/422/485) Audio: x1 DC-input: x1 (12V DC-in JACK)	
RAID	Non RAID, RAID 1	Non RAID, RAID 1, 5, 6	
Electrical	Input Voltage: 12VDC, 5A Power Supply: 43W	Input Voltage: 12V / 4A Power Supply: 48W	Input Voltage: 12V / 7.5A Power Supply: 90W
Operating Environment	Temperature: 5° C to 40° C Humidity: 5% to 80% (non-condensing)		
LED Indicator	Yes (Network, System, HDD)	Yes (Network, System, HDD, Fan/ Temperature)	
Dimensions (mm)	190(H) x 110(W) x 245(D) mm	225(H) x 175(W) x 245(D) mm	
Weight (without hard drives)	3kg (without HDD)	5kg (without HDD)	
Certificate	FCC / CE Class A		
Warranty	3 years		

	SMR8300E Series	SMR8300A Series
System Processor	Intel Core i3 Dual Core 3.3GHz	Intel Core i7 Quad Core 3.4GHz
System Memory	DDR3 4GB (up to 16GB)	
Operating System	Linux Embedded System	
Storage	3.5" SATA HDDs x8	
	HDD hot swappable with LED status indicator	
I/O Interface	RJ-45: 2x Gigabit Ethernet USB: 6x USB2.0 VGA(DVI): x1 HDMI: x1 COM: x1	
RAID	Non RAID, RAID 1, 5, 6	
Electrical	Input Voltage: 100-240 V, 3.5A Power Supply: 430W	
Operating Environment	Temperature: 5° C to 40° C Humidity: 5% to 80% (non-condensing)	
LED Indicator	Yes (Network, System, HDD)	
Dimensions (mm)	310(H) x 175(W) x 380(D) mm	
Weight (without hard drives)	8.9kg (without HDD)	
Certificate	FCC / CE Class A	
Warranty	3 years	

1.2.2. VMS Specifications

Live View	<ul style="list-style-type: none"> • Real-time network camera discovery • Versatile views of various screen divisions • Multiple views supported • View patrolling for single or multiple views • Real time video/event alarm display • Support 3 installation modes and 5 different fisheye Dewarp display modes • Support live audio
eMAP	<ul style="list-style-type: none"> • Drag-n-drop camera manipulation • Hierarchical map structure • Real time event alert • Instant live video of camera
PTZ	<ul style="list-style-type: none"> • Pan, tilt, zoom operations (dependent of the camera) • Built-in, floating PTZ control panel • Preset position (dependent of the camera) • Event-driven camera patrolling
I/O	<ul style="list-style-type: none"> • Digital I/O management
Multiple Displays	<ul style="list-style-type: none"> • Support dual monitors • Supports live view, playback, eMap functions • Direct display to secondary monitor(s)
Investigation	<ul style="list-style-type: none"> • Search by date, time, camera • Search by VI event combinations • Search over multiple days • Search over multiple cameras • Different color display on recorded data date • Search via built-in VI analyzer • Intuitive, video thumbnail search results • Cue-in, cue-out and repeat • Quick playback by video thumbnail • 1/8, 1/4, 1/2, 1x, 2x, 4x, 8x play, pause, stop • AVI-formatted video clip export • Up to 16 channel synchronized playback (depends on product) • Support 3 installation modes and 5 different Fisheye Dewarp playback display modes
Video Intelligence	<ul style="list-style-type: none"> • General motion detection • Camera motion detection • Missing object detection • Foreign object detection • Intrusion detection • Forbidden area detection • Tampering detection • Virtual Fence • Go in/out detection (configure on remote client) • Tailgating detection (configure on remote client)
Recording Policy	<ul style="list-style-type: none"> • Supports up to 64 channels megapixel recording • Continuous recording • Event-driven recording along with rules • Scheduled recording on daily or weekday basis • Post alarm recording 1-300 seconds • Pre-alarm recording 1-300 seconds
Rule Manager	<ul style="list-style-type: none"> • Conditional recording/alert/notification • Email, FTP, SMS, popup window, PTZ,VI Panel, Relay output notifications • Sound, alarm, round-the-clock alerts
Remote Management	<ul style="list-style-type: none"> • Full functional operation & management via VMS Client • Remote management and control via SCC & SCC Client

Remote Client	<ul style="list-style-type: none"> • Web Client • iPhone Client • Android Client
3rd Party IPCAM	<ul style="list-style-type: none"> • Support ONVIF • ACTi, Arecont Vision, Axis, Dahua, Dynacolor, Hikvision, IQinvision, Mobotix, Panasonic, and more
Storage Expansion	<ul style="list-style-type: none"> • Built-in RAID storage management
General & Misc	<ul style="list-style-type: none"> • Video privacy mask • Digital zoom in, zoom out • Log viewer, log export mechanism • Client auto login • Automatic storage recycling • Client-server architecture • Customized authority account management • Configurable video retention period • Digital watermark proofing • Support DDNS Function • Support time sync with NTP time server • Provide System and VI setup Help assistance • Support Customized Event Management and log mechanism • Auto port mapping for internet connection
Language	<ul style="list-style-type: none"> • Multiple Language supported on VMS and Web Client: Czech, Dutch, French, German, Italian, Japanese, Korean, Persian, Polski, Portuguese, Russian, Slovak, Spanish, Turkish, Simplified Chinese, Traditional Chinese

Chapter 2. Hardware Overview

2.1 Front Panel

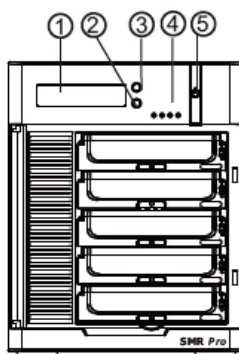
Front View

SMR2100
SMR2110



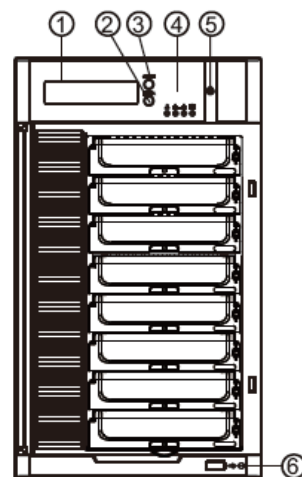
- ① LCD Display
- ② Enter Switch

SMR5110



- ③ Select Switch
- ④ LED Indicators

SMR8300

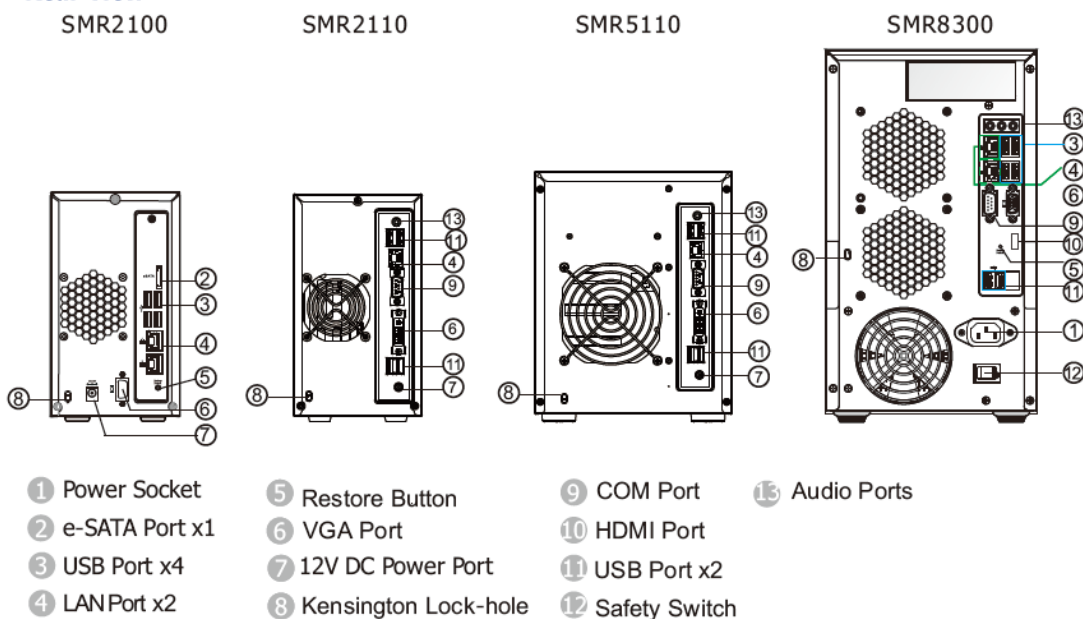


- ⑤ Power Switch
- ⑥ Front USB Connector

	Function
1. LCD Display	Connect the display
2. Enter Switch	Use this switch for confirmation
3. Select Switch	Use this switch for selection
4. LED Indicators	Indicates the status
5. Power Switch	Powers up the system
6. Front USB Connector	Connects external accessories such as mouse, keyboard or other external devices.

2.2. Rear Panel

Rear View



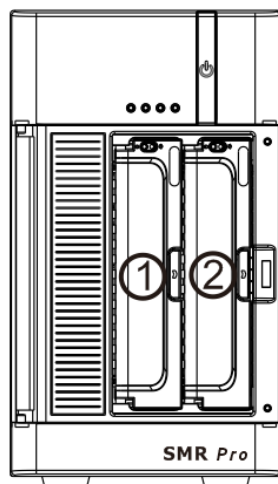
	Function
1. Power Socket	Used for connecting power cable.
2. e-SATA Port x1	Used for connecting the SMR with e-SATA drives.
3. USB Port x4	Used for exporting video clips as evidence support to external storage devices.
4. LAN Port x2 (GbE Ethernet port)	Used for connecting the system with the network. Note that for single LAN Mode, use LAN1
5. Restore Button	Use for reset the system to factory default. For details, please refer to the table below.
6. VGA Port	Used for attaching an external monitor to the system.
7. 12V DC Power Port	Used for connecting power cable.
8. Kensington Lock-hole	For use with a Kensington lock. Please refer to your Kensington lock for instructions.
9. COM Port	Used for connecting various devices, such as a mouse, modem, network, printer and so on.
10. HDMI Port	Used for connecting audio/video devices such as video projectors and DVD players.
11. USB Port x2	Used for exporting video clips as evidence support to external storage devices.
12. Safety Switch	Used for preventing injury if someone inadvertently attempts to open the machine. Please make sure it's on after the power cable is attached to the power socket.
13. Audio Ports	Used for attaching audio devices such as headphones and speakers.

2.3. Hard Drive Designation

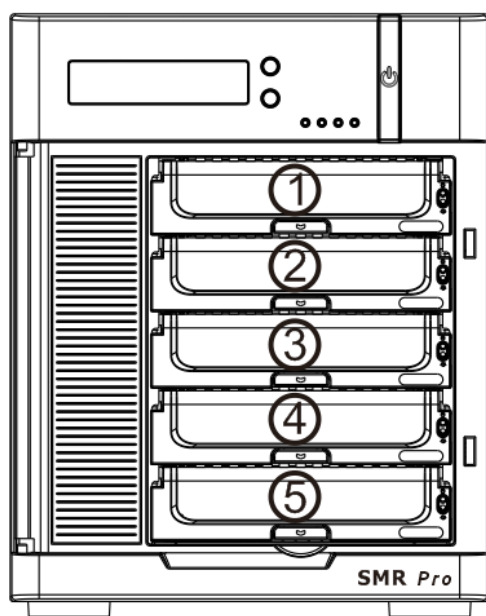
Hard disk drives are purchased separately. When selecting hard disk drives (HDD), HDD manufacturers always urge users to choose enterprise/surveillance grade drives for 24/7 surveillance operations to ensure system stability. The surveillance hard drives on our Approved Vendor List (AVL) are engineered to work continuously, withstand high-temperature fluctuations and equipment vibrations found in any typical surveillance application. To reduce errors occurred on your RAID data and the chance of the recording performance being affected, it is highly recommended to use HDDs listed on our Approved Vendor List (AVL) to ensure reliability. Find the AVL on our web page: <http://www.surveon.com/support/hardware.asp>

The hard drive arrangement for each system is shown below. The general alignment is from left to right and/ or top to bottom in numeric order.

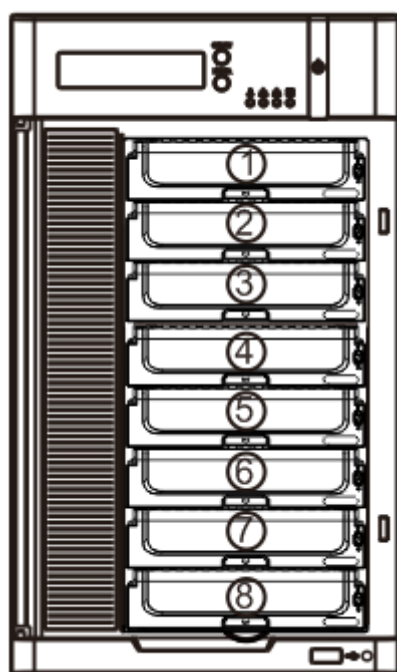
SMR2000 Series



SMR5000 Series

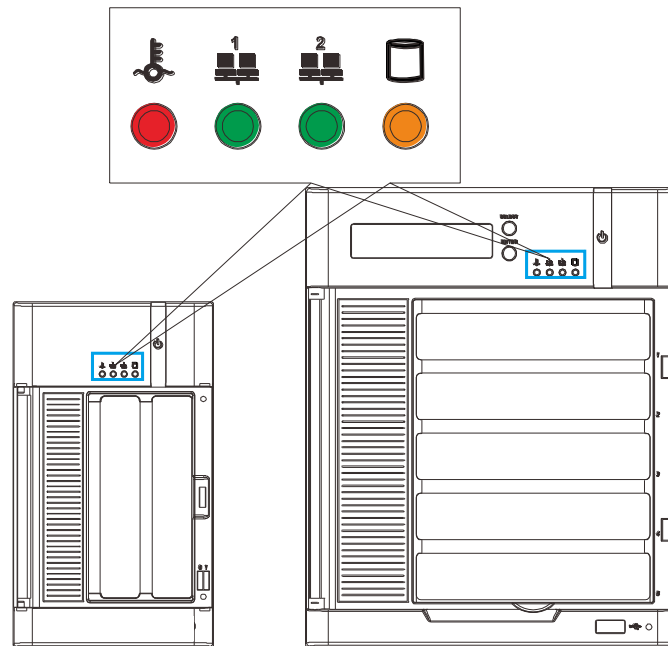










SMR8000 Series



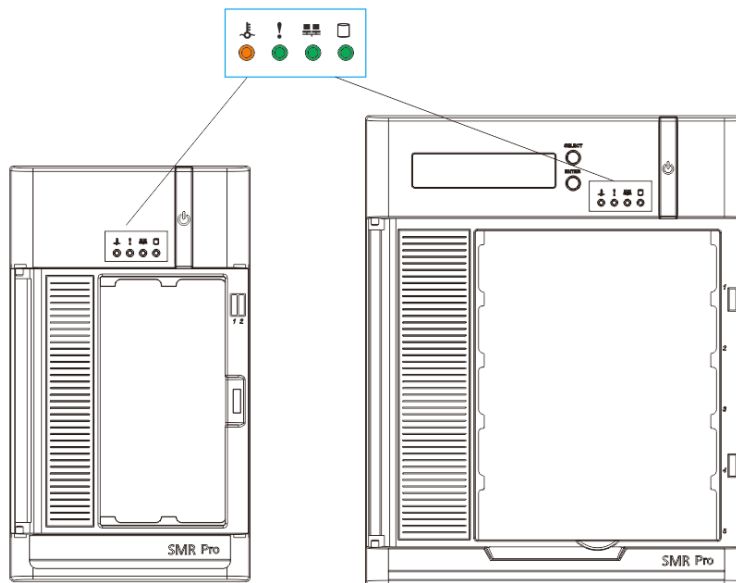
2.4. LED Definitions









2.4.1. Desktop System Front Panel LEDs for SMR2100, SMR8300



Name	Color	LED Status	Function
Network    	Green	On	Indicates that power is on and network is connected.
		Off	Indicates that network is disconnected.
		Blink	Indicates that network activity is in progress.
HDD  	Amber	On	Indicates that the hard drive can be accessed.
		Off	Indicates that a hard drive read/write error occurred.
		Blink	Indicates one of the followings: (1)Disk volume creation is in progress. (2)Online RAID level migration is in progress. (3)RAID rebuilding is in progress.
System  	Red	On	Indicates the system fan is malfunctioning.
		Blink	Indicates that system is starting up.

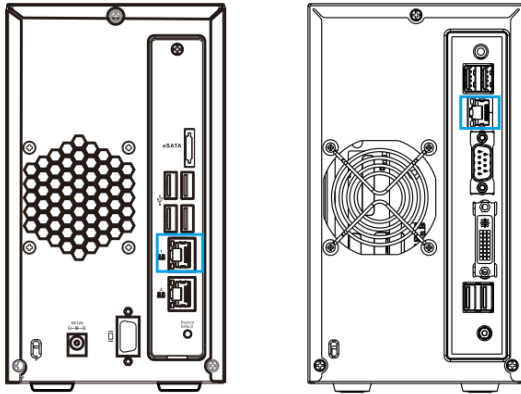
2.4.2. Desktop System Front Panel LEDs for SMR2110, SMR5110



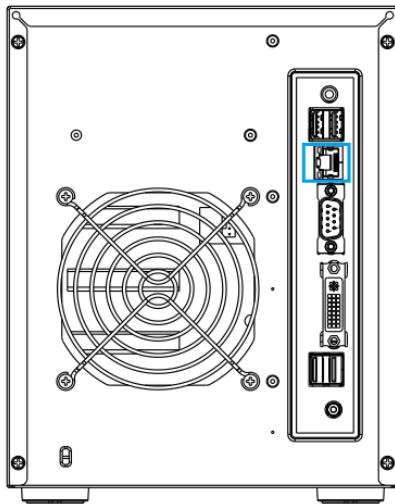
	Name	Color	LED Status	Function
 	Temperature / Fan Status	Amber	On	Indicates overheat/Fan fail
			OFF	Indicates normal
 	System Status	Green	Green (Normal)	Normal operation
		Amber	Amber(Fail)	System failure (RAID failed/error, Disk failed, NVR Server, or the Stream Server Service stop)
 	Network Status	Green	Flashing	Indicates network activity
 	HDD Status	Green	Flashing	Indicates HDD activity

2.4.3. Rear Panel Ethernet LED

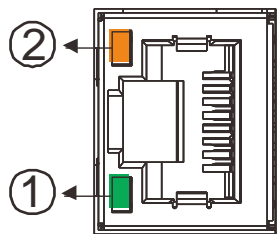
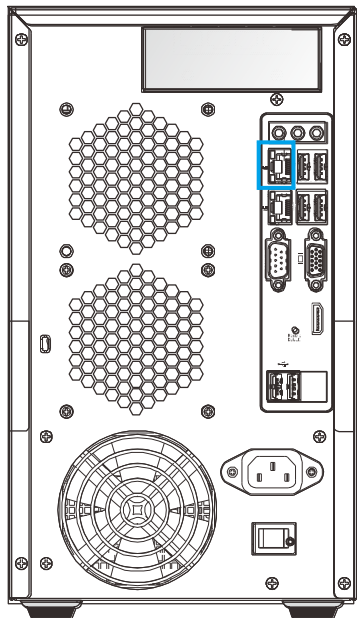
SMR2000 Series



5000 Series



8000 Series



Name	Color	LED Status	Function
1. Link Status LED	Green	On	Indicates that the connection is established.
		Off	Indicates that the connection is not established.
2. Activity LED	Amber	Blink	Indicates data transfer activity

Chapter 3. Software Overview

3.1. Software Introduction

Video Management Software (VMS) is a highly modular and powerful video and hardware management suite that incorporates Server recording, management, and video monitoring and playback functionalities to serve the core purposes of a video surveillance system.

It operates in a client-server mode: The Local Client and Local Domain Server run for standalone SMR/NVR/VMS Server, while the Remote Client receives live video streams and event video playbacks from LAN or Internet. All administrative tasks are performed on the Client. The client software provides the ability to monitoring and playback recorded videos from multiple cameras. And for users having multiple SMR/NVR/VMS Servers, Surveon Control Center (SCC) (its main functions are the same with the VMS) can be utilized to manage over the domain infrastructure.

3.2. Module Framework

- VMS/NVR Server
 - Combines video recording, archival and retrieval functionalities for individual servers/standalone PCs.
 - Serves as the connection point for client stations.
- Local Domain Server
 - The interface between the VMS/VI Servers and any clients.
 - User authentication server.
- Local Client
 - Local access, VMS Client installed on standalone PCs/NVRs for live video monitoring, event recording playback access and VMS system configuration.
- Remote Client (full functions)
 - Remote access, VMS Client installed on remote PCs for live video monitoring, event recording playback access.
 - Serves as the default configuration point for NVR2000 series, which do not have a Local Client.
- Web Client (for simple use)
 - Remote access, an ActiveX application (OCX) installed on remote PCs for live viewing and event playbacks through the web browser.
- SPhone Client (for simple use)
 - SPhone Client installed on iOS/ Android devices for basic live viewing.
- Web Server
 - Allows user to access the live video stream, PTZ control and event recording playbacks through Microsoft Internet Explorer 7.0 (or higher) after the Web Clients components are downloaded.
- VI Server
 - The video intelligence processing point for a VMS solution.
 - Preinstalled on SMR/NVR Server, and optional on a separate server/PC (VMS).
- SCC Domain Server
 - Allows centralized control over multiple Trusted VMS Server points and connections from multiple clients.
- SCC Client

- Software capable of accessing multiple Trusted VMS Servers through the SCC Domain Server

3.3. System Architecture

VMS operates in scalable client - server architecture. This architecture can be divided into three types: (1) Standalone Server (2) Standalone Server + Remote Client (Web Client/SPhone Client) (3) Multiple Servers + SCC Client.

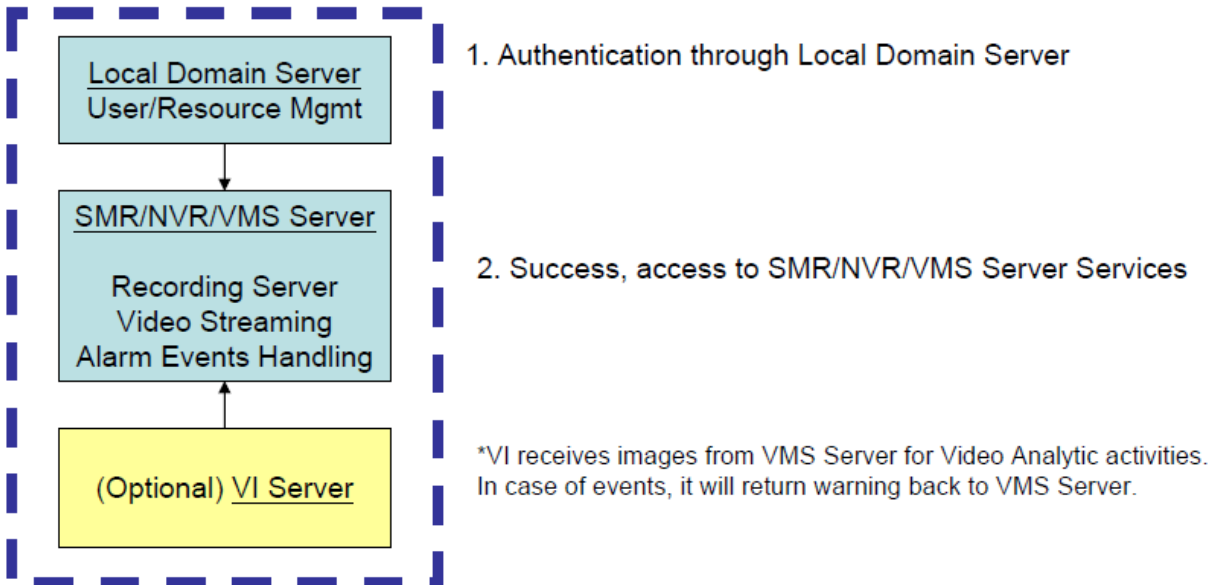
These are the hardware requirements for using PCs as Server or Client.

VMS Server + Client			
Support NVRs	≥ 32CH	16~32CH	≤ 16CH
OS	64-bit : Windows 7 Professional, Enterprise, Ultimate		
CPU	Intel Core i7-980X or above	Intel Core i7-860 or above	Intel Core i5-650 or above
Memory	4 GB or above		
Display	nVidia GeForce GTX660 2GB or above		
Hard Drive	SATA 7200 RPM, 500 GB or above		
Network	1 Gbps or above		
Remote Client			
OS	64-bit : Windows 7 Professional, Enterprise, Ultimate		
CPU	Intel Core i7-980X or above	Intel Core i7-860 or above	Intel Core i5-650 or above
Memory	4 GB or above		
Display	nVidia GeForce GTX660 2GB or above		
Hard Drive	SATA 7200 RPM, 500 GB or above		
Network	1 Gbps or above		
VMS Server Only			
OS	64-bit : Windows 7 Professional, Enterprise, Ultimate		
CPU	Intel Core i3-530 or above		
Memory	4 GB or above		
Display	On board (generic) 256MB or above		
Hard Drive	SATA 7200 RPM, 500 GB or above		
Network	1 Gbps or above		

3.3.1. Standalone Server (Client-Server All-in-One)

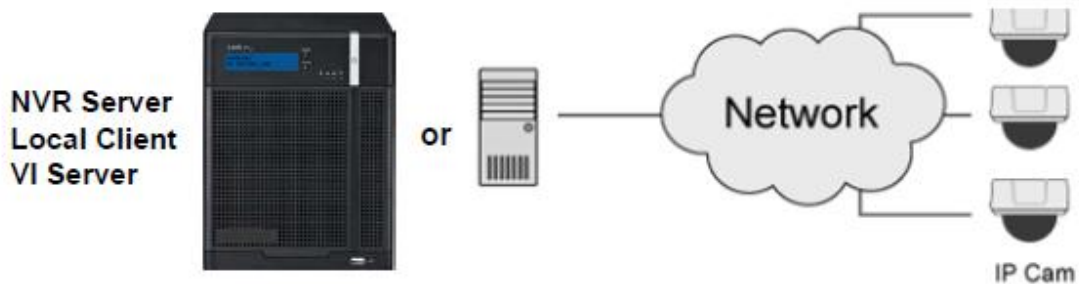
For users with standalone Server, the Local Client UI is used to manage NVR Server services:

Local Client UI



※Application:

The Server, IP cameras are all in the same LAN.



Use NVR as Server

No installation needed.

Use PC as Server

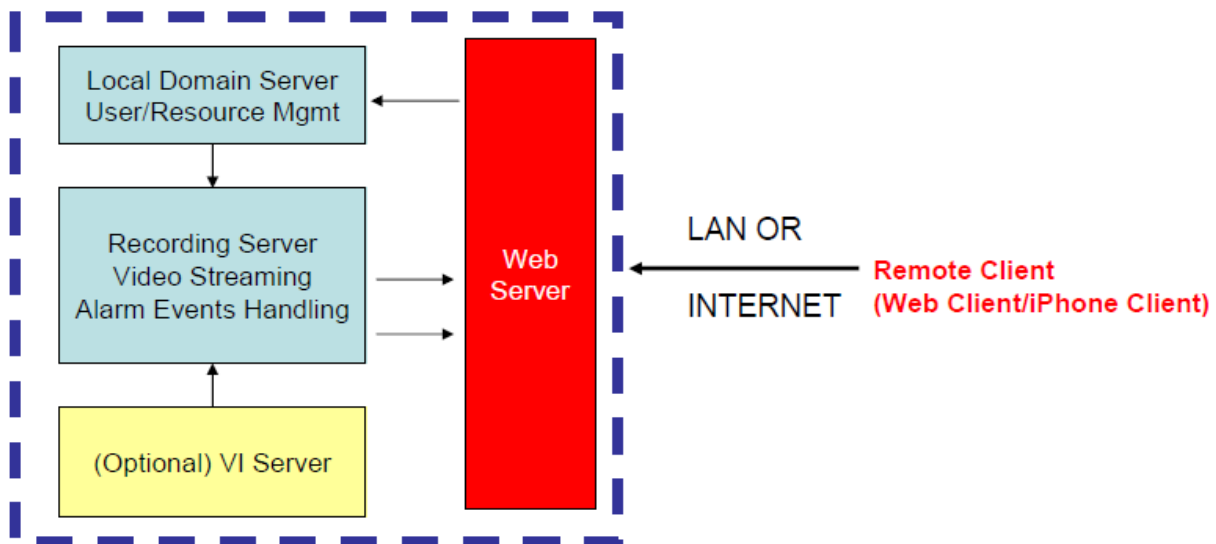
Install both the VMS/NVR Server and VMS Client on a PC:

①Insert the VMS/IPCAM product CD. ②Click **VMS Suite** on the menu to start the installation. ③Choose *Typical Setup*. If you don't need video analytic functions, *Advanced Setup* can be selected to uncheck the VI Server.

3.3.2. Standalone Server + Remote Client (Web Client / SPhone Client)

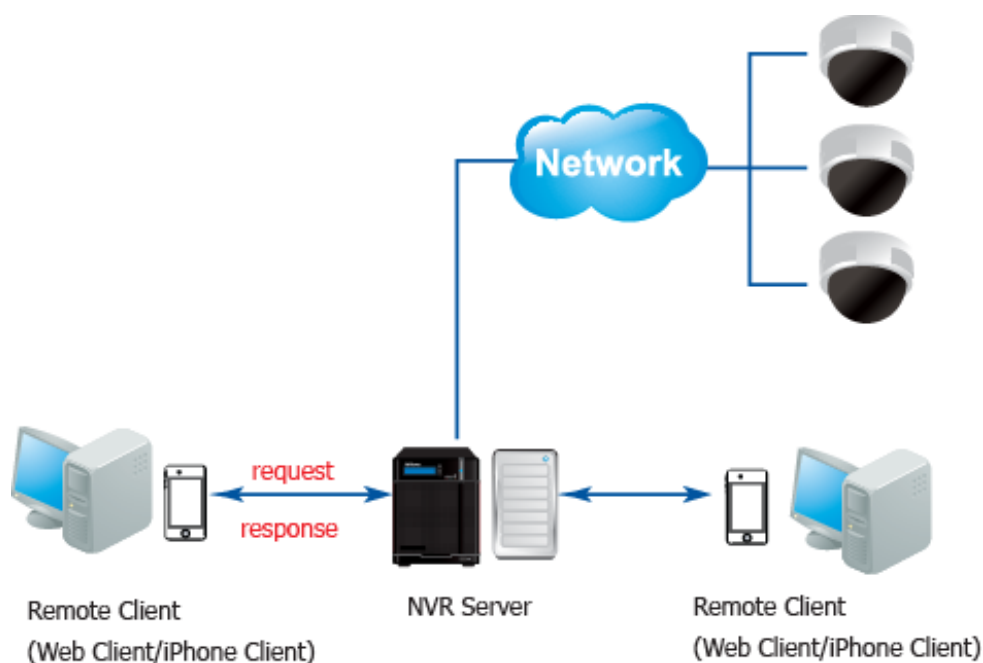
For remote users to connect to SMR/NVR Server, a remote access, VMS Client installed on remote PCs is needed for live video monitoring, event recording playback access.

Also, the Web Client, an ActiveX application (OCX) can be used for basic live viewing and event playbacks through the web browser, while SPhone Client can be used for basic live viewing on iPhone/Android devices.



Application1: Internet

The Server, IP cameras and the PC/Mobiles are all in the same LAN.



[NVR Server]

Use SMR/NVR as Server

No installation needed.

Use PC as Server

Install the VMS/NVR Server on a PC:

- ① Insert the VMS/IPCAM product CD.
- ② Click **VMS Suite** on the menu to start the installation.
- ③ Choose *Advanced Setup* to uncheck the VMS Client.

If you don't need video analytic functions, the VI Server can also be unchecked.

Install the Web Server on the PC:

- ① Insert the VMS/IPCAM product CD.
- ② Click **Browse CD/DVD** in the menu.
- ③ Double click **WebServerSetup.exe** to start the installation.

[Client]

Install the VMS Client on PCs:

- ① Insert the NVR/SMR product CD.
- ② Click **VMS Client** on the menu to start the installation.

Install the Web Client on the PCs (Optional):

Launch Microsoft Internet Explorer 7.0 (or above) and enter your **VMS Server IP address + "/webclient"** in your web browser's URL location, eg. <http://172.18.6.9/webclient> to download the Web Client application.

Install the SPhone Client (Optional):

Download the SPhone Client from App Store on the iPhone desktop.

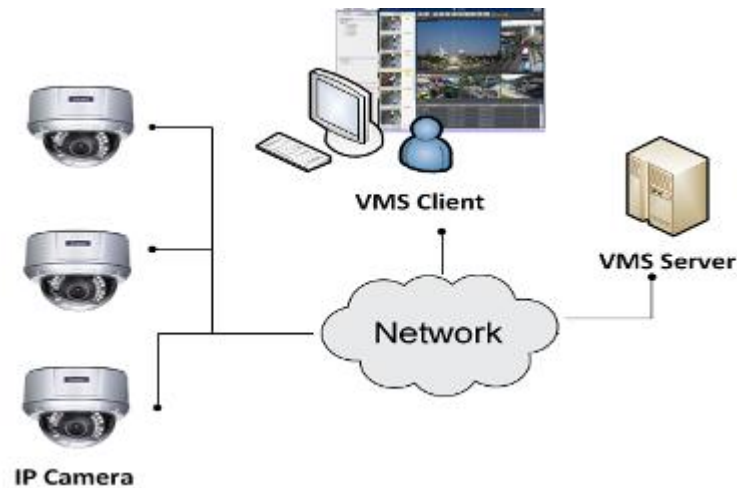
Install the SPhone Client (Optional)

Download the SPhone Client from App Store on the Andriod phone desktop.

Note: Please refer to *Installing the VMS* and *Installing the Web Client* for details.

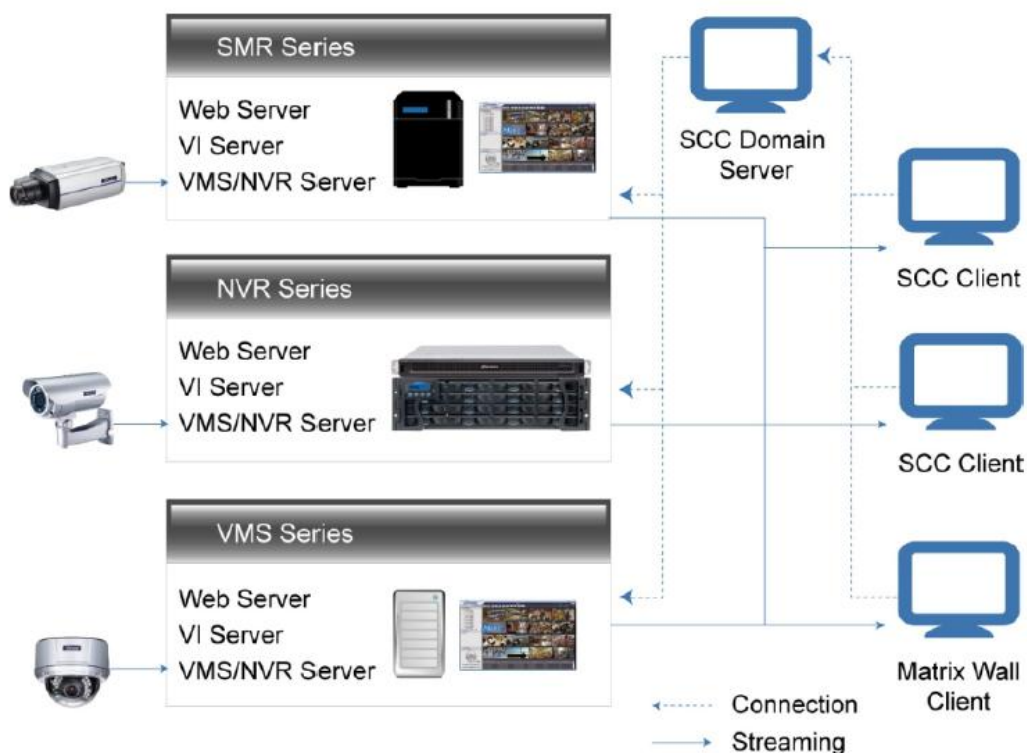
Application 2: Internet

The Server, some of the IP cameras and the PC are all in the same LAN, while the other IP cameras are installed in remote location with Public IP.



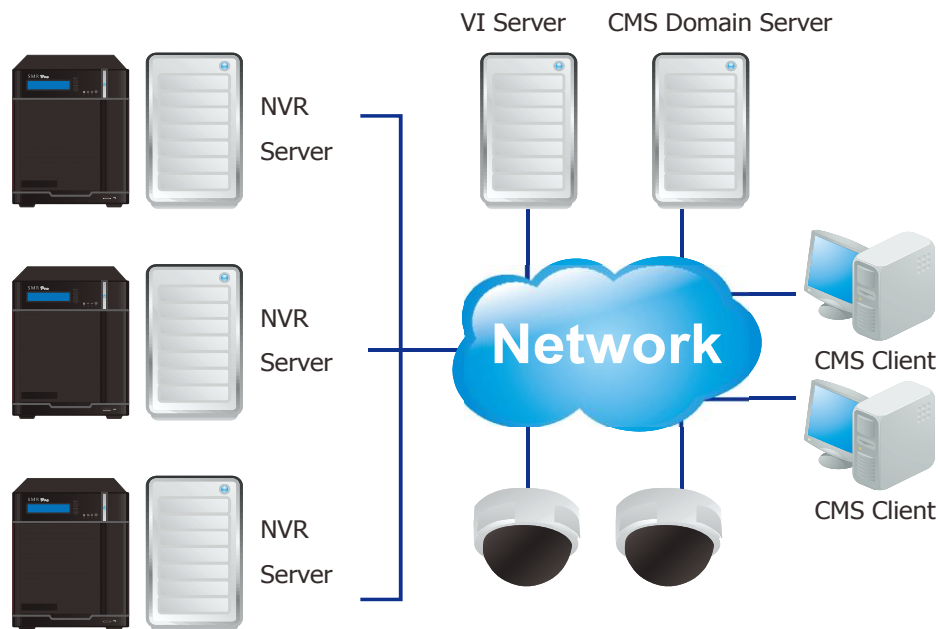
3.3.3. Multiple Servers + SCC Client

For users with multiple SMR/NVR Servers, SCC Client UI is used to manage over the domain infrastructure.



Application3: Internet

- (1) The Servers, IP cameras and the PCs are in LAN A.
- (2) Some IP cameras are installed in LAN B, which is behind a different router in a remote location.
- (3) Users are allowed to connect the SMRs/NVRs from remote PC over the Internet.



[NVR Server]

Use SMR/NVR as Server

No installation needed.

Use PC as Server

Install the VMS/NVR Servers on PCs:

- ① Insert the VMS/IPCAM product CD.
- ② Click **VMS Suite** on the menu to start the installation.
- ③ Choose *Advanced Setup* to uncheck the VMS Client.

The VI Server can also be unchecked, if you don't need video analytic functions.

[VI Server] (Optional)

You can choose to install the VI Server only on a standalone PC to manage the video intelligence data.

- ① Insert the VMS/IPCAM product CD.
- ② Click **VMS Suite** on the menu to start the installation.
- ③ Choose *Advanced Setup* to choose VI Server only.

[SCC Domain Server]

Install the SCC Domain Server on a PC:

- ① Insert the NVR/SMR product CD.
- ② Click **SCC Suite** on the menu to start the installation.
- ③ Choose *Advanced Setup* to select the SCC Domain Server only.

[SCC Client]

Install the SCC Client on PCs:

- ① Insert the NVR/SMR product CD.
- ② Click **SCC Suite** on the menu to start the installation.
- ③ Choose *Advanced Setup* to select the SCC Client only.

Note: (1) For users don't have Surevon SMR/NVR series, please contact your dealer for the SCC installation file. (2) The SCC Domain Server can also be installed together with the SCC Client in the same PC by choosing *Typical Setup*. (3) Please refer to *Installing the VMS* and *Installing the SCC* for details.

3.3.4. Network Requirements

In order to preserve enough bandwidth for surveillance video, a surveillance network is presumed to be free of user/business traffic. Server software currently supports Class B and Class C type addresses. Currently the Server software only searches for Servers on the same subnet. Cameras should also reside on the same subnet.

Opening Ports

If access through a firewall in a local network is required, try opening the following ports: SMTP (25), HTTP (80), FTP (20, 21), OMNI (2809), HTTPS (443) and RTSP (554, 8554.). Other ports should also be opened while using port forwarding to access the VMS Server: Stream Port (9090), Doman Data Port (9060), Log Download Message Port (15507) and Log Download Data Port (9080).

Access through a firewall	Use port forwarding to access
SMTP (25), HTTP (80), FTP (20, 21), OMNI (2809), HTTPS (443), RTSP (554, 8554.)	Stream Port (9090), Doman Data Port (9060), Log Download Message Port (15507), Log Download Data Port (9080)

Note: Please refer to *Port Forwarding* Section for more details.

Warnings / Precautions

If the Server and a VMS client reside on separate subnets, please set up gateway, VLAN, or cross-subnet routing to bridge surveillance traffic. Please consult with a network administrator for problems with network setups. A VMS client needs to be rebooted when network settings are changed.

3.4. Port Forwarding

Port forwarding is a name given to the combined technique of:

1. Translating the address and/or port number of a packet to a new destination.
2. Possibly accepting such packet(s) in a packet filter (firewall).
3. Forwarding the packet according to the routing table.

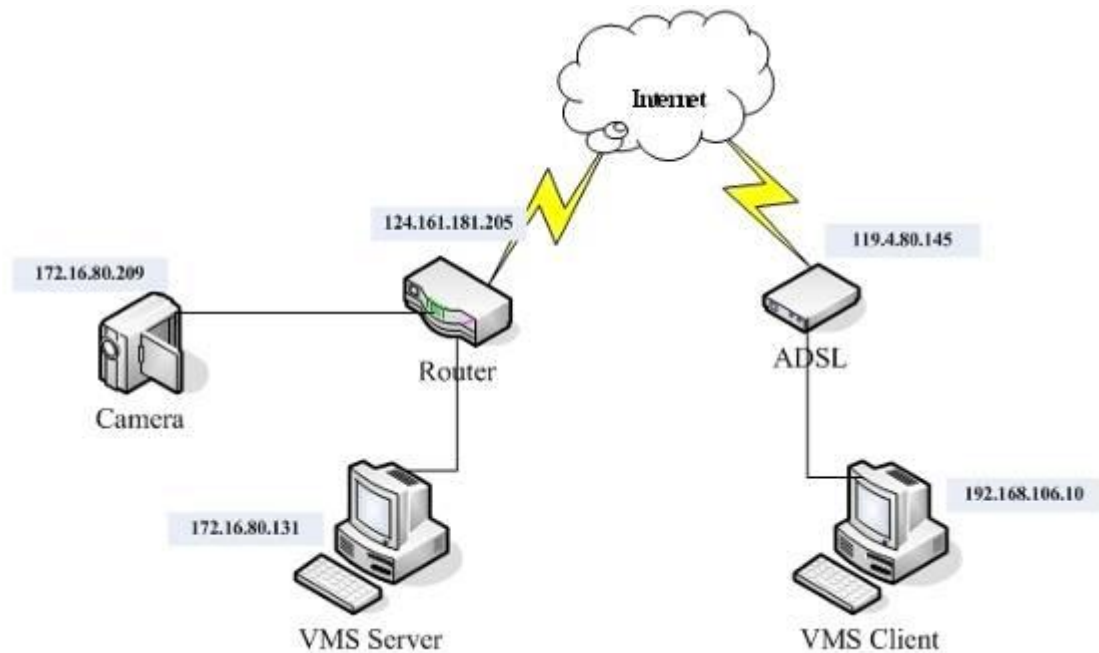
To illustrate its concept, two computers on the Internet that communicate with each other using TCP/IP or UDP/IP protocols(though the process is not limited to these) utilize ports to identify the opposite connection points of each other where the data packets supposed to go to. In order to communicate, each computer knows the port of another computer (in addition to IP address) and sends the data to that port. Port forwarding forwards these ports in such a way that when one computer sends data to the specific port of another computer, the data is actually sent to a different port. This allows remote computers to connect to a specific computer or service within a private LAN.

In a typical residential network, nodes obtain Internet access through a DSL or cable modem connected to a router or network address translator (NAT/NAPT). Hosts on the private network are connected to an Ethernet switch or communicate via a wireless LAN. The NAT device's external interface is configured with a public IP address. The computers behind the router, on the other hand, are invisible to hosts on the Internet as they each communicate only with a private IP address.

When configuring port forwarding, the network administrator sets aside one port number on the gateway for the exclusive use of communicating with a service in the private network, located on a specific host. External hosts must know this port number and the address of the gateway to communicate with the network-internal service.

When used on gateway devices, a port forward may be implemented with a single rule to translate the destination address and port. The source address and port are, in this case, left unchanged. When used on machines that are not the default gateway of the network, the source address must be changed to be the address of the translating machine, or packets will bypass the translator and the connection will fail.

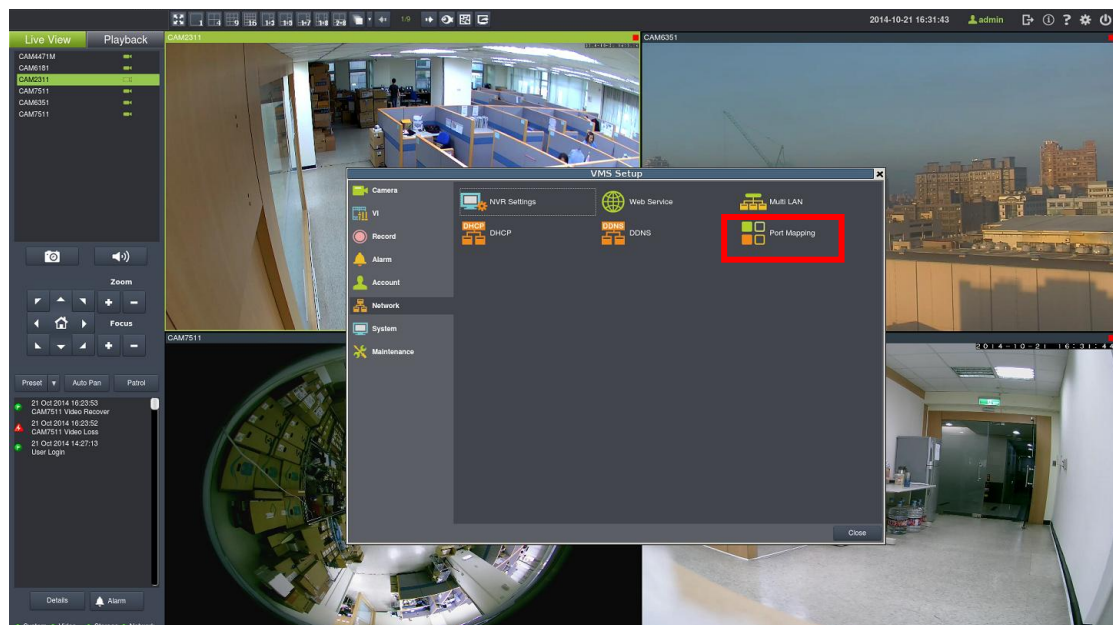
3.4.1. Port Forwarding for Accessing VMS Server



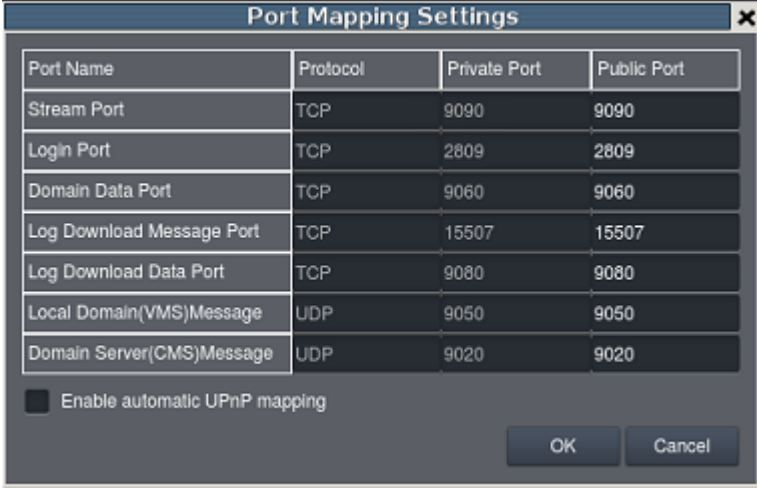
To enable port forwarding for accessing VMS Server, please follow the steps below:

1. Do Router Port Mapping for VMS/SMR Server

Go to **VMS Setup > Network > Port Mapping** in VMS after it is installed.



A *Router Port Mapping* window will prompt for entering port numbers. Please put in the numbers as listed below:



The screenshot shows a window titled "Port Mapping Settings" with a close button (X) in the top right corner. Inside the window is a table with four columns: "Port Name", "Protocol", "Private Port", and "Public Port". The table contains eight rows of data. Below the table is a checkbox labeled "Enable automatic UPnP mapping" which is currently unchecked. At the bottom right of the window are two buttons: "OK" and "Cancel".

Port Name	Protocol	Private Port	Public Port
Stream Port	TCP	9090	9090
Login Port	TCP	2809	2809
Domain Data Port	TCP	9060	9060
Log Download Message Port	TCP	15507	15507
Log Download Data Port	TCP	9080	9080
Local Domain(VMS)Message	UDP	9050	9050
Domain Server(CMS)Message	UDP	9020	9020

☐ Enable automatic UPnP mapping

OK Cancel

Stream Port: 9090

Login: Port: 2809

Doman Data Port: 9060

Log Download Message Port: 15507

Log Download Data Port: 9080

2. Open Ports on the Router

Host Ports: The private ports that the internal VMS/SMR Server use, which are unchangeable.

Global Ports: The public ports for remote clients to connect to the internal VMS/SMR Server. The Global ports are changeable, but the simplest way is to make them the same with the host ports.

Please open the listed ports on your router:

(When the option “Enable Automatic Upnp Mapping” is selected, this step can be skipped.)

Port(Host/Global Port)	Protocol	Port Number
Domain Message Port	UDP	9050
Domain Data Port	TCP	9060
Login Port	TCP	2809
Stream Port	TCP	9090
Log Download Message Port	TCP	15507
Log Download Data Port	TCP	9080

Web Management Platform

Dynamic NATOne-to-one NATInternal ServerApplication Layer InspectionConnection Limit

Create Internal Server

InterfaceCellular0/0

ProtocolTCPUDP

Global IP AddressCurrent Interface IP Address

Global PortOther (0-65535, 0 represents any.)

Host IP Address

Host PortOther (0-65535, 0 represents any.)

Add

Select the internal server(s) you want to remove

Interface	Global IP Address	Global Port	Host IP Address	Host Port	Protocol
Ethernet0/0	current-interface((0.0.0.0))	9060	192.168.1.2	9060	TCP
Ethernet0/0	current-interface((0.0.0.0))	9050	192.168.1.2	9050	UDP
Ethernet0/0	current-interface((0.0.0.0))	2809	192.168.1.2	2809	TCP
Ethernet0/0	current-interface((0.0.0.0))	15507	192.168.1.2	15507	TCP
Ethernet0/0	current-interface((0.0.0.0))	9080	192.168.1.2	9080	TCP
Ethernet0/0	current-interface((0.0.0.0))	9090	192.168.1.2	9090	TCP
Ethernet0/0	current-interface((0.0.0.0))	9050	192.168.1.2	9050	UDP

Select AllSelect None

Delete

Note: Camera port (default: 80) and stream port (default: 6002) for accessing cameras should be opened while VMS/SMR Server and the cameras and are not in the same LAN.

Chapter 4. Installation

4.1. Before You Start

4.1.1. Checklist for Operating Environment

Users need to prepare the following devices to set up the surveillance system.

Network Video Recorder	THE SYSTEM series
IP Camera	Network Cameras (such as CAM2441)
Network	Existing LAN, Switch, Router or Hub (please see the Network Topology below)
Storage	Hard Drives

Note: The hard drives should be purchased separately.

4.1.2. Checklist for Network Topology

Make sure you have the right switch/hub for your environment. Either of the following options will work.

	Common Topology	Reference Product
Existing LAN	LAN Switch with DHCP Server	Office LAN
Router	LAN Switch with build-in DHCP Server	D-Link DIR-130
Switch/Hub	No DHCP Server(refer to the Note below)	D-Link DES-1108

Note: For devices without DHCP Server function, please refer to Configuring DHCP Service Section.

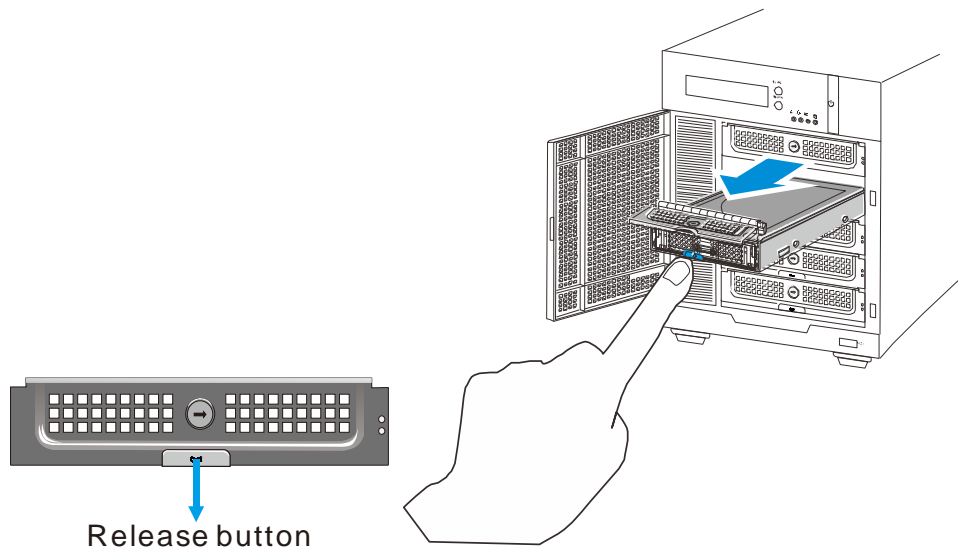
4.2. Hard Drive Installation

4.2.1. Hard Drive Installation Prerequisites

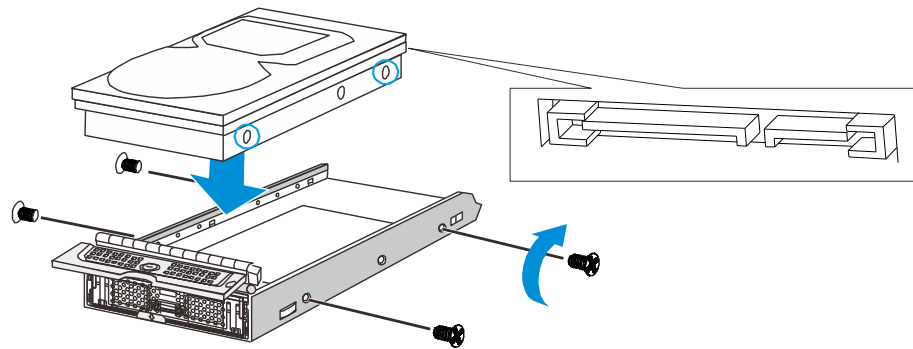
Purchase hard drives having the same capacity and using same interface with the pre-installed ones.

4.2.2. Inserting Hard Drive into Drive Tray (Desktop Series)

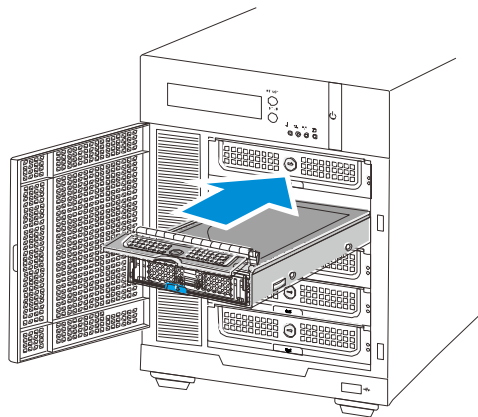
1. Open the front panel of the SMR system.
2. Press the release button (indicated by the **blue arrow**) on the bezel, the bezel panel should open automatically and gently pull out the hard drive tray.



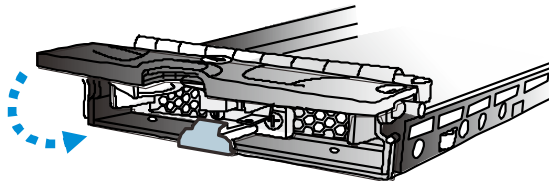
3. Place the hard drive into the drive tray. Make sure the hard drive's interface connector is facing the open side of the drive tray and its label side facing up. Adjust the drive's location until the mounting holes in the drive tray are aligned with those on the hard drive. Secure the drive with four supplied flat head screws.



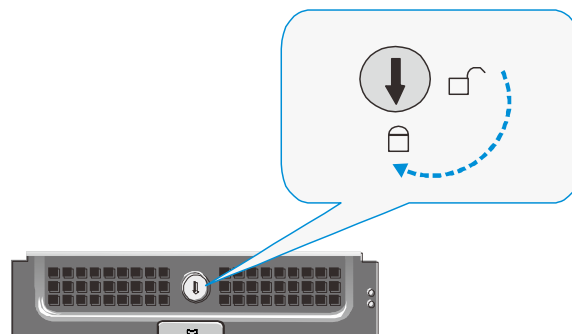
4. With the tray bezel open, insert the hard drive and tray into the system enclosure.



5. Close the tray bezel.

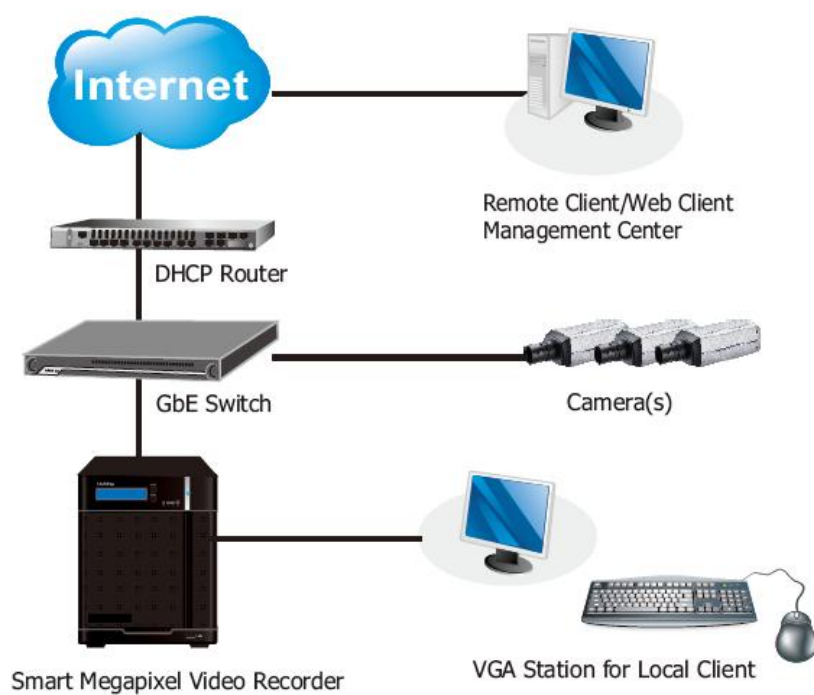


6. Use the small flat blade screwdriver to turn the bezel lock from the unlock to lock position.

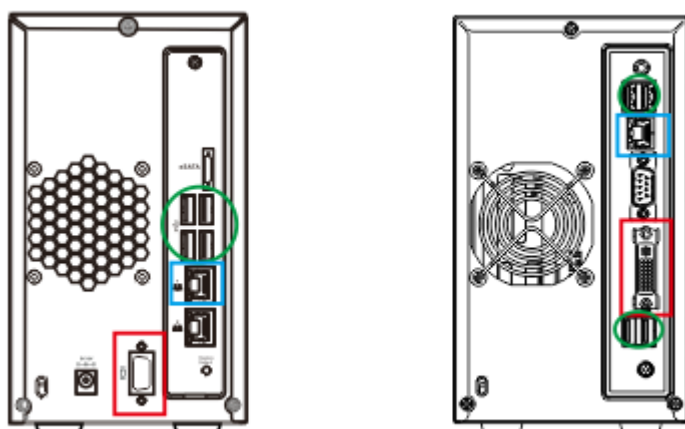


7. Repeat above steps to install other hard drives.
8. Close the system front panel when you are done installing hard drives.

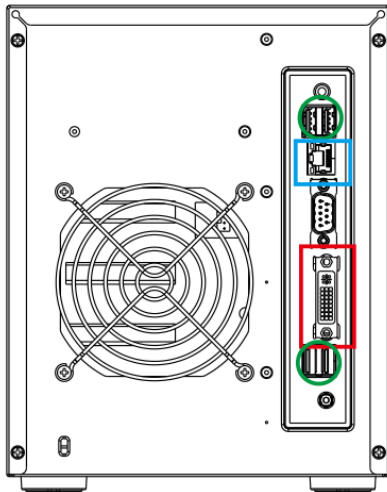
4.3. System Connections



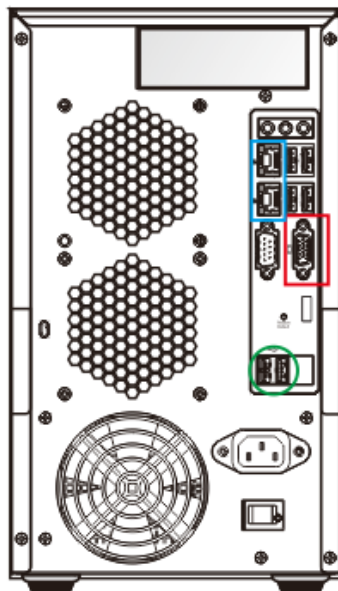
Connect cables to the rear panel ports as follows:
SMR2000 Series



5000 Series






8000 Series

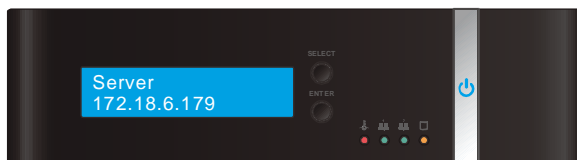


- Insert mouse, keyboard or other external devices to the USB port (green circles) for operating the Video Management Software (VMS).
- Insert the LAN cable to the upper LAN port (blue rectangles) to connect the SMR to a local network where your IP cameras reside.
(Connection to analog cameras is also available via an IP encoder.)
- Connect an external monitor capable of 32bit or higher color quality to the VGA Port (red rectangles) to view the VMS interface.

4.4. Powering up SMR

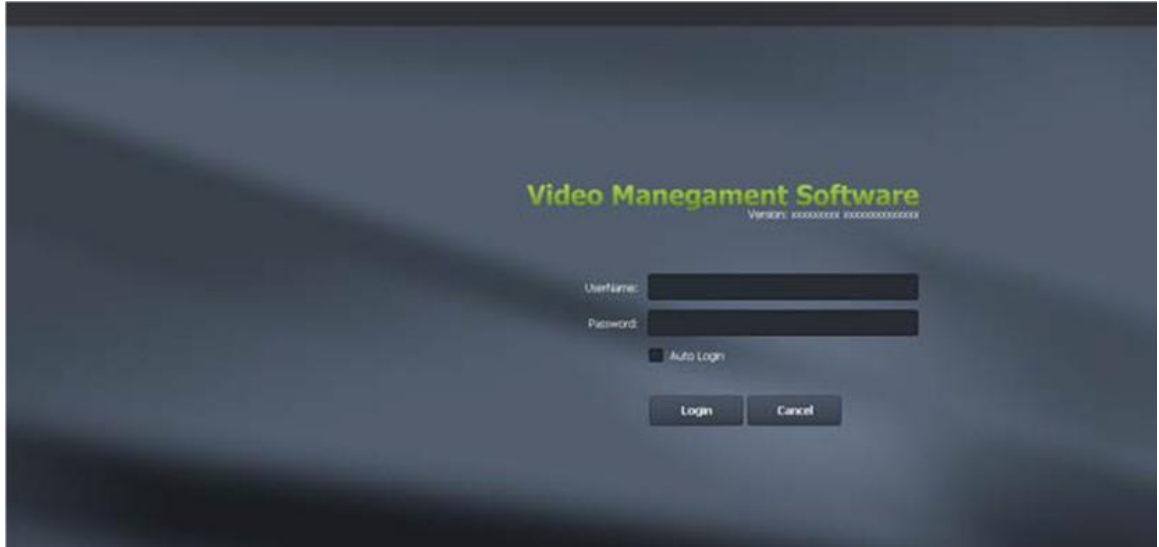
4.4.1. SMR Systems

1. Attach the power cable to the power socket on the rear panel.
2. (SMR8000 Series) Make sure the safety switch on the rear panel is switched to the “-” side, which means that it is turned on.
3. Press the Power Switch.
4. See if the System LED  is blinking, which means the system is starting up.
5. See if the Network LED  has turned green, which indicates power is on and network is connected.
6. See if the HDD LED  is on, which means the hard drive can be accessed.
7. (SMR8000 series) The Server name and the IP address will be shown on the LCD screen.



4.5. Logging into SMR Series

The Local Client will prompt for the following information after the system Series system is powered on:



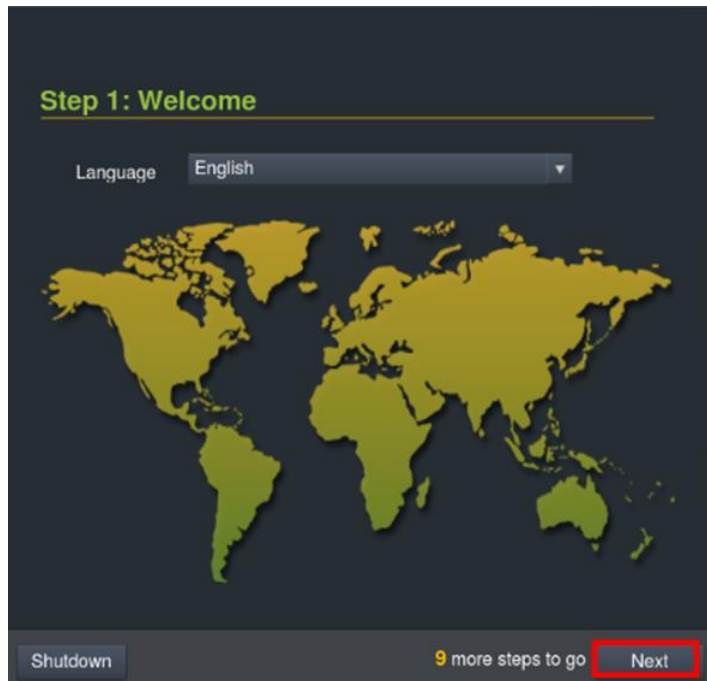
- **Username:** The username of the domain, which is always admin.
- **Password:** The password of the domain. Default password is admin.
- **Auto Login:** Check this option and you do not have to input the username and the password again when logging in next time.

Click Login after the password is entered.

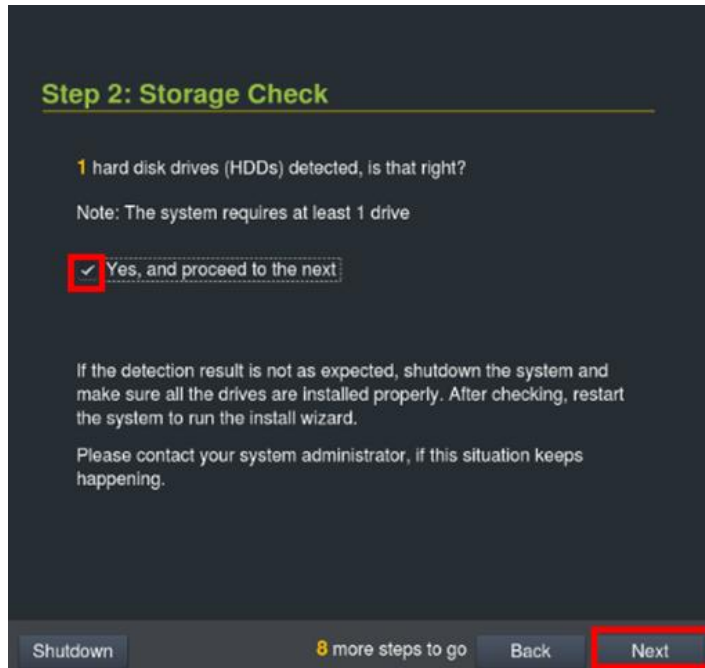
4.6. Run the Install Wizard

When you run the system series for the first time, you need to go through the following steps within the Install Wizard after logging in.

1. Welcome: Use the dropdown list to select the language for the VMS. Click **“Next”** to go to the next step **Storage Check**.



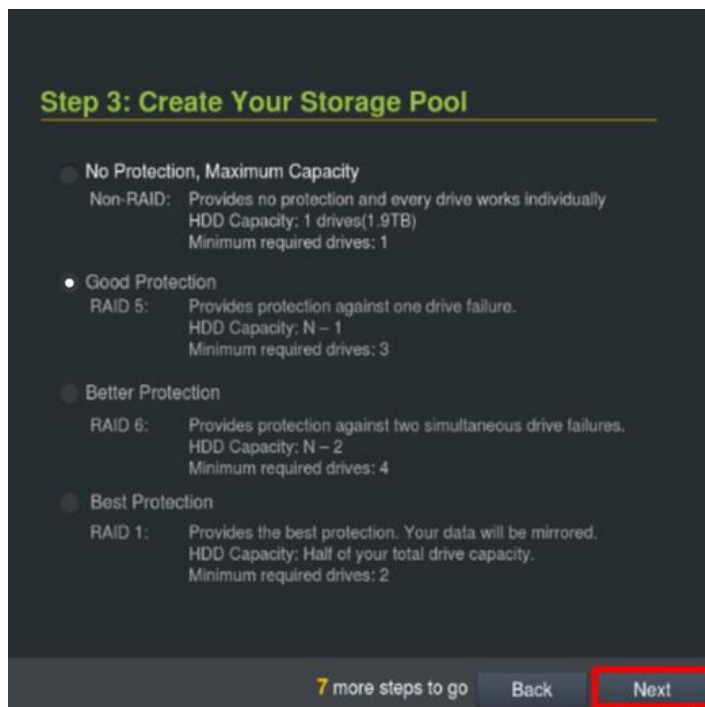
2. Storage Check: the system will auto detect the number of installed hard disk drives. Check if the detection result is correct, if yes, check **”Yes and proceed to the next step”**. Click **“Next”** to go to the next step **Create Your Storage Pool**.



If the detection result is not as expected, shutdown the system and make sure all the drives are installed properly. After checking, restart the system to run the install wizard.

Contact your system administrator, if this error occurs again.

3. Create Your Storage Pool: Select the best storage configuration for the system.



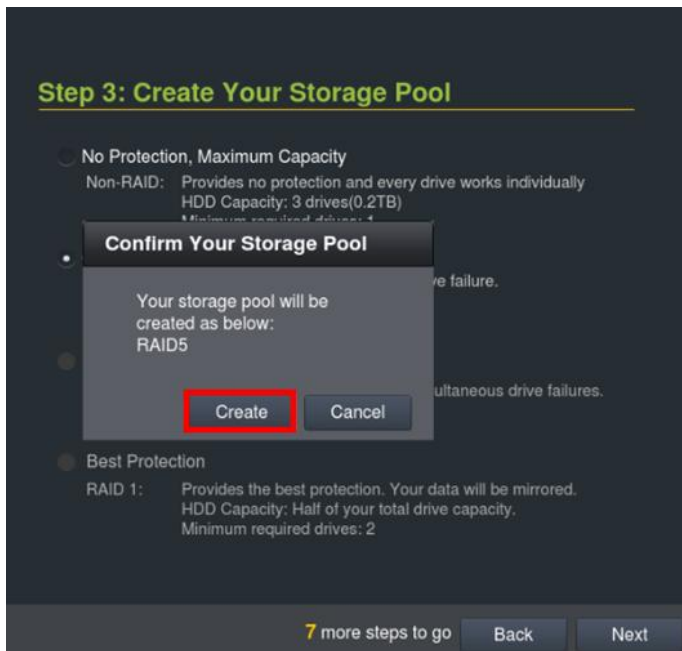
These are the RAID options.

RAID Level			
RAID	Description	Min. HDD	HDD Used for Storage
No Protection, Maximum Capacity (Non-RAID)	No protection, but maximum capacity.	2	All of HDDs
Good Protection (RAID 5)	Use 1 disk to store the parity function data to provide fault tolerance.	3	HDD number minus 1
Better Protection (RAID 6)	Used 2 disks to store the parity function data to provide fault tolerance.	4	HDD number minus 2
Best Protection (RAID 1)	Best protection. Your data will be mirrored.	2	Half of HDDs

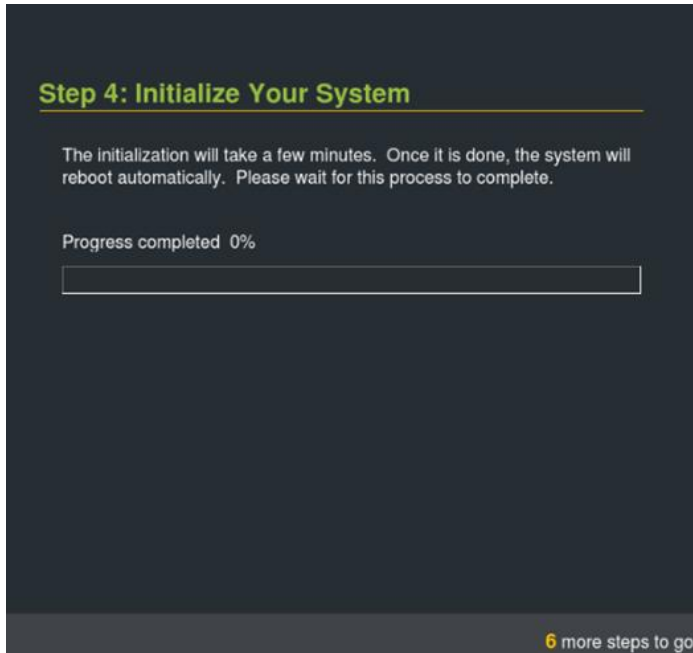
Please seek for professional help, if you are not sure how to select the RAID level.

3.1. After the selection is done, a confirmation will be prompted as below.

Click “Create”, if the statement shown is correct.



4. **Initialize Your System:** This act will take a few minutes to complete. Once it is done, the system will reboot automatically.



5. System Basic Settings: You can change or use the default password.

Check the “**Use Default Password**” option, if you wish to keep the default password.

If you want to change the password, input a new password and confirm the newly created password.

Click “**Next**” to go to the next step **Setup Time**.

Step 5: System Basic Settings

Server Name

Administrator Account Settings

Username

☒ Use Default Password

Password

Confirm Password

5 more steps to go **Next**

6. Setup Time: Time setup should be done correctly, otherwise some of the functions will be affected. Set up the time zone before setting up the time. Click “**Next**” to go to the next step **Recording Policy**.

Step 6: Setup Time

Time Zone (GMT +8:00) Beijing, Perth, Singapore, Hong ▼

Time 2014-10-21 15:27:46 ▼

Tip: You need to setup the time zone first and then set the time up accordingly.

4 more steps to go Back Next

Note: Date / Time should be set correctly before recording.

7. Recording Policy: Select the best profile for your scenario to have a balanced resource usage for the quality of recording and local display.

- When **“Always recording”** is selected, every image will be recorded.
- When **“Motion recording”** is selected, only motion detected images will be recorded, and approximately 25%~60% of storage can be saved according to the levels of motion detection you have set.

Recording and Local Display Profile Selection:

- When **“Standard mode”** is selected, the system will not set limitations on the recording and local display.
- When **“High Quality Viewing Mode”** is selected, the system will suppress the resources on the local display to have the recording quality enhanced.
- When **“Recording Capacity Maximized Mode”** is selected, the system will close the resources on the local display to maximize the recording quality.

Click **“Next”** to go to the next step **Setup Your Network**.

Step 7: Recording Policy

- **Always Recording**
All cameras record 24/7 continuously.
- **Motion Recording**
All cameras record when any motion is detected.

Recording and Local Display Profile

- **Standard mode**
The video quality will be fair for both recording videos and local display.
- **High Quality Viewing Mode**
The video quality is better while the local display capacity will be suppressed.
You may use the remote client for a better viewing quality.
- **Recording Capacity Maximized Mode**
Compromise the local display quality to maximize the recording capacity.

3 more steps to go Back **Next**

8. Setup Your Network:

Tick the option **“Obtain An IP Address Automatically”**. The system will detect your network environment automatically to see if there is a DHCP server and generate an IP address for you.

You can also select **“Input The IP Address Manually”** to set up the IP address manually.

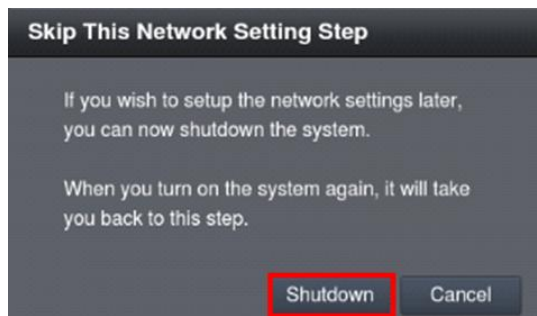
Make sure there is no DHCP server in the network environment before ticking the option **“Auto Assign IP Address For Cameras (Make this NVR as a DHCP server)”** to make this SMR as a DHCP server. Ask your IT engineer for help, if you are not sure how to set up.


Click **“Next”** to go to the next step **Add Cameras**.

You can click **“Skip”** if you wish to set up the network settings later.

After selecting **“Skip”**, a confirmation window will appear. Click **“Shutdown”** to turn off the system.

When you turn on the system, it will take you back to this step.

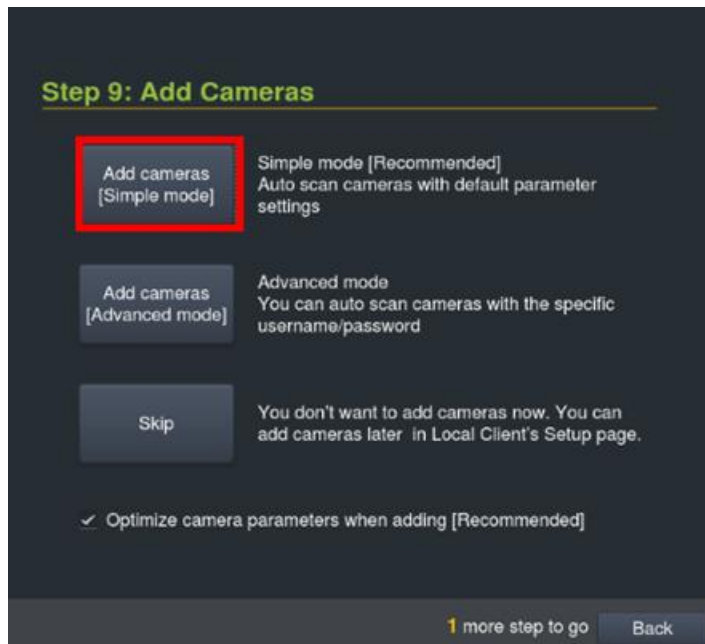


 **Warning:** Make sure that only 1 DHCP server is activated in your system, otherwise it may cause network errors.

Note: You can also change the network settings, once you're logged in to the Local Client. Go to *Setup > Network > DHCP Server* for the network configuration.

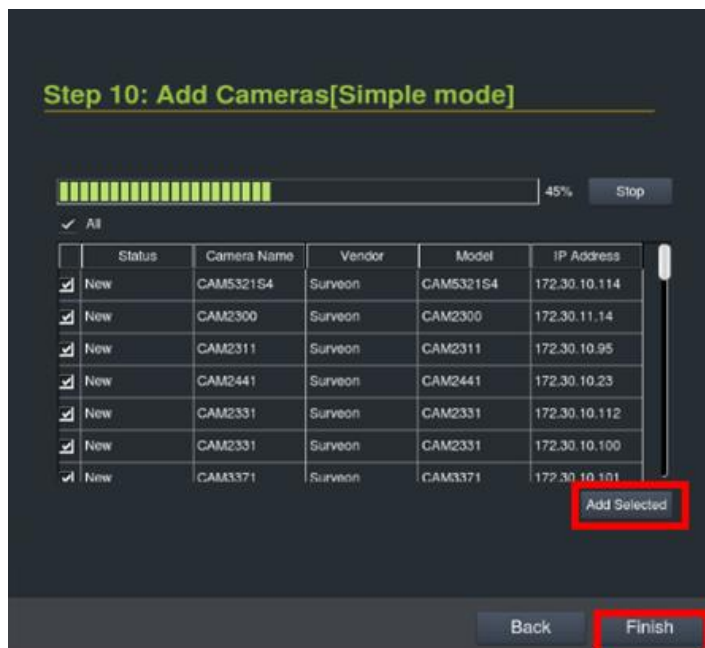
9. Add Cameras

Select “Add Cameras [Simple Mode]” to add cameras by auto scan.



After selecting, you will see the list of connected cameras.

Select the cameras you'd like to add and select “Add Selected” and then click “Finish” to complete the installation and exit the Wizard.



Note: You may reboot the cameras to refresh their IP addresses from the DHCP server, if some of the IP addresses are shown the same or the cameras can not be reached.

or “Add Cameras [Advanced Mode]” to add cameras by auto scan and with editable parameters.

Step 9: Add Cameras

Add cameras [Simple mode]

Simple mode [Recommended]
Auto scan cameras with default parameter settings

Add cameras [Advanced mode]

Advanced mode
You can auto scan cameras with the specific username/password

Skip

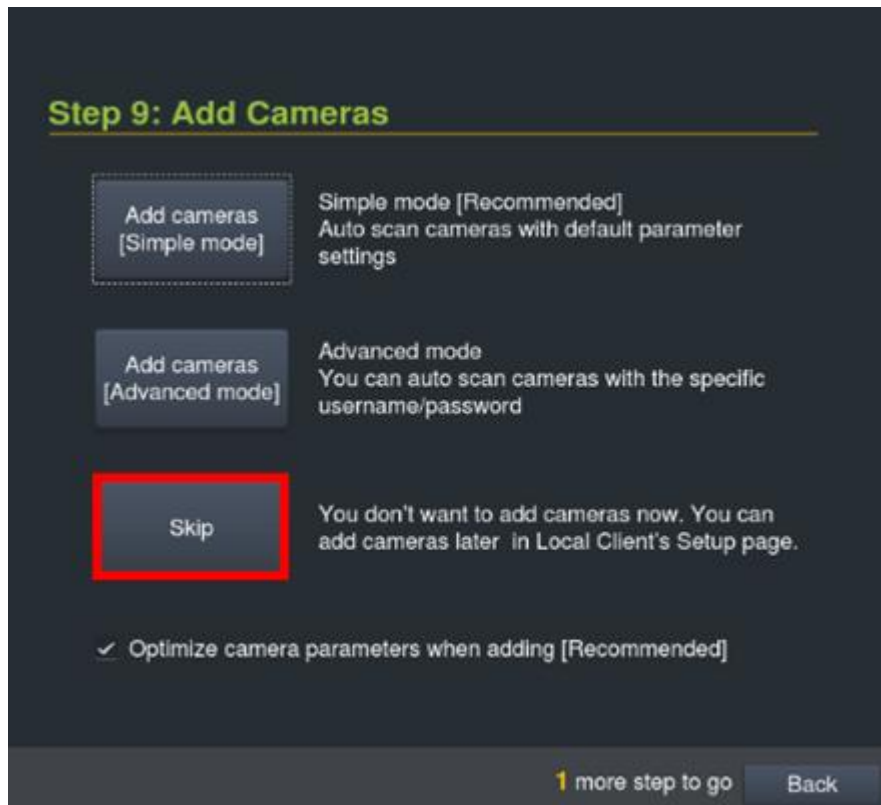
You don't want to add cameras now. You can add cameras later in Local Client's Setup page.

☒ Optimize camera parameters when adding [Recommended]

1 more step to go Back

Scan For Cameras										
Status Scanning										45% Stop
	Status	Camera Name	Vendor	Model	IP Address	Username	Password	Http Port	Stream Port	MAC Address
<input checked="" type="checkbox"/>	New		ONVIF	ONVIF	11.130.11.1	admin	*****	80	554	
<input checked="" type="checkbox"/>	New	ACTI	ACTI	E32A	172.30.10.110	admin	*****	80	7070	000F7C0E
<input checked="" type="checkbox"/>	New	ACTI	ACTI	E53	172.30.10.126	admin	*****	80	7070	000F7C0E
<input checked="" type="checkbox"/>	New	CAM532154	Surveon	CAM532154	172.30.10.114	admin	*****	80	6002	00226000
<input checked="" type="checkbox"/>	New	CAM2300	Surveon	CAM2300	172.30.11.14	admin	*****	80	6002	00D02360
<input checked="" type="checkbox"/>	New	CAM1320	Surveon	CAM1320	172.30.11.12	admin	*****	80	6002	00D02360
<input checked="" type="checkbox"/>	New	CAM4311	Surveon	CAM4311	172.30.11.15	admin	*****	80	6002	00D02360
<input checked="" type="checkbox"/>	New	CAM2311	Surveon	CAM2311	172.30.10.95	admin	*****	80	6002	00D02360
<input checked="" type="checkbox"/>	New	CAM4371	Surveon	CAM4371	172.30.10.105	admin	*****	80	6002	00D02360
<input checked="" type="checkbox"/>	New	CAM2311P	Surveon	CAM2311P	172.30.11.1	admin	*****	80	6002	00D02360
<input checked="" type="checkbox"/>	New	CAM2441	Surveon	CAM2441	172.30.10.23	admin	*****	80	6002	00D02360
<input checked="" type="checkbox"/>	New	CAM2331	Surveon	CAM2331	172.30.10.112	admin	*****	80	6002	00D02360
<input checked="" type="checkbox"/> Select/Deselect All		Username	admin	Password	*****	Http Port	80	Stream Port	6002	Apply All
		<input type="button" value="Ok"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>								

You can also click **“Skip”** to leave this step, if you wish to add cameras later in the **Local Client’s Setup** page.



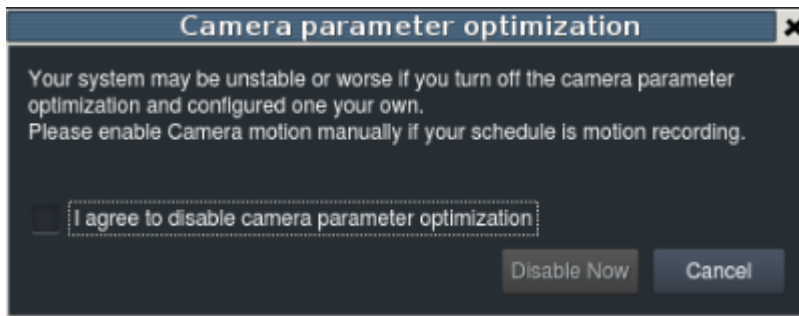
Click **“Skip”** , a window will prompt to ask for confirmation.



Click **“Shutdown”** to shutdown and start from this step next time.

Click **“Finish”** to close this window and the system will be directed to the **Local Client**.

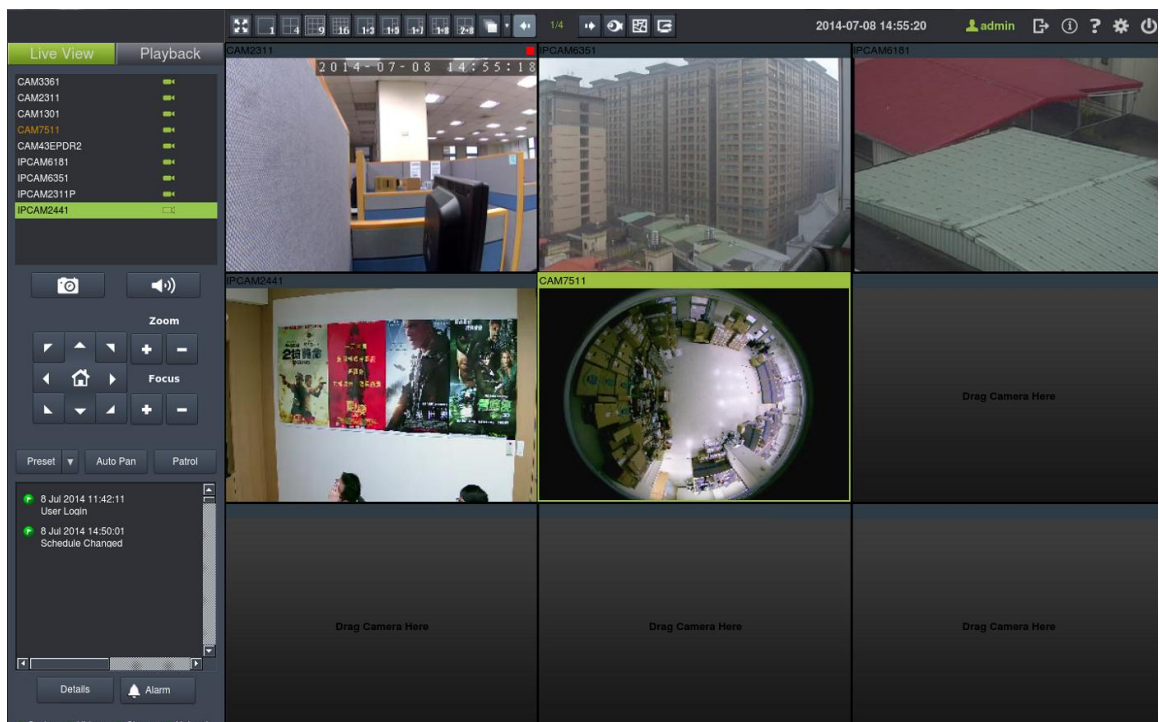
When the option **“Optimize camera parameters when adding”** is not selected, a warning will show up, confirming your wish not to optimize the cameras. Check the option **“I agree to disable camera parameter optimization”** if you really to skip the camera optimization.



Note: The cameras can also be added, after logged in to the **Local Client**.
Refer to the **Local Client** user manual Chapter 5.2. Adding Cameras to the Server for more details.

Note: After the installation is done, the system will optimize the connected cameras and the settings of resolution, FPS and bit rate might be different from your operation plan. In this case, please change the camera setting after adding camera.

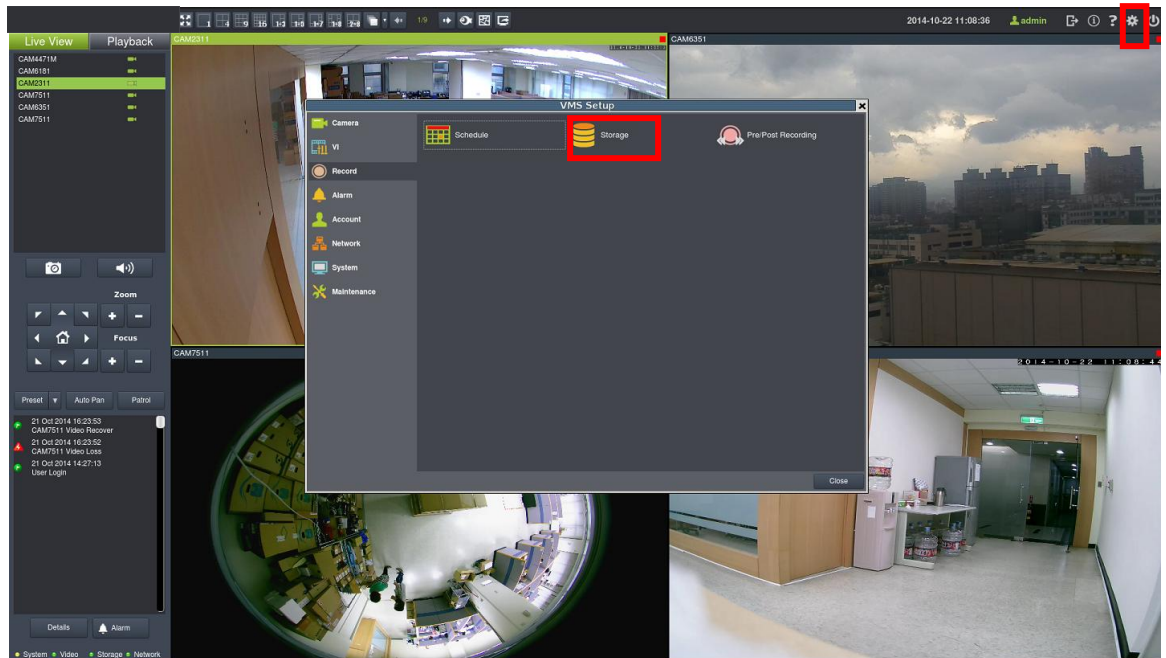
After the wizard installation is done, you will see the **Live View** page from the **Local Client**. Please refer to its user manual for the system Series Local Client Operation.



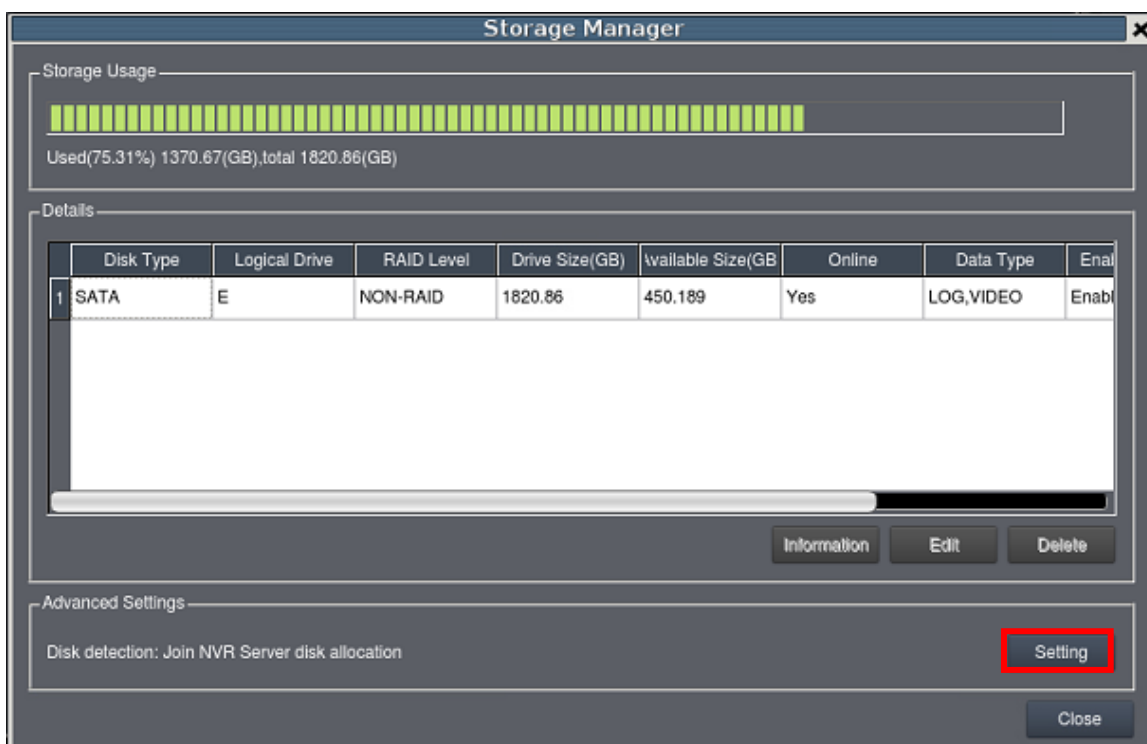
Chapter 5. Basic System Settings

5.1. Storage Management

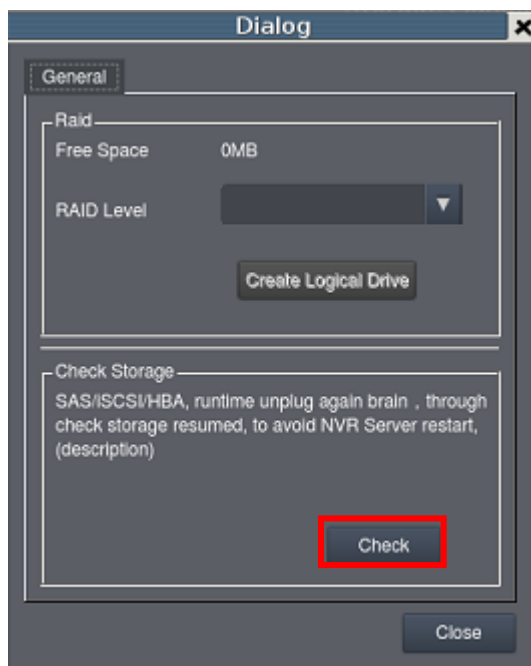
1. To access the information about the drives configured in your Server, click **Setup** to bring out **VMS Setup** window and then select **Recording** to see and click **Storage** option for **Storage Manager**.



2. All available Logical Drives, as well as their sizes, free space, and status will appear. Click target drive and then **Setting** to set the log and location for saving the video recordings.



3. Click the target drive first and then **Settings**. In "General" tab, click **Check**.



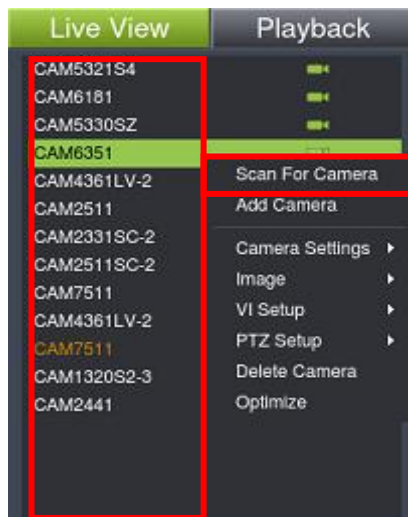
4. Choose the RAID level, and then click **Create Logical Drive** to create the RAID configuration.

5.2. Adding Cameras to the Server

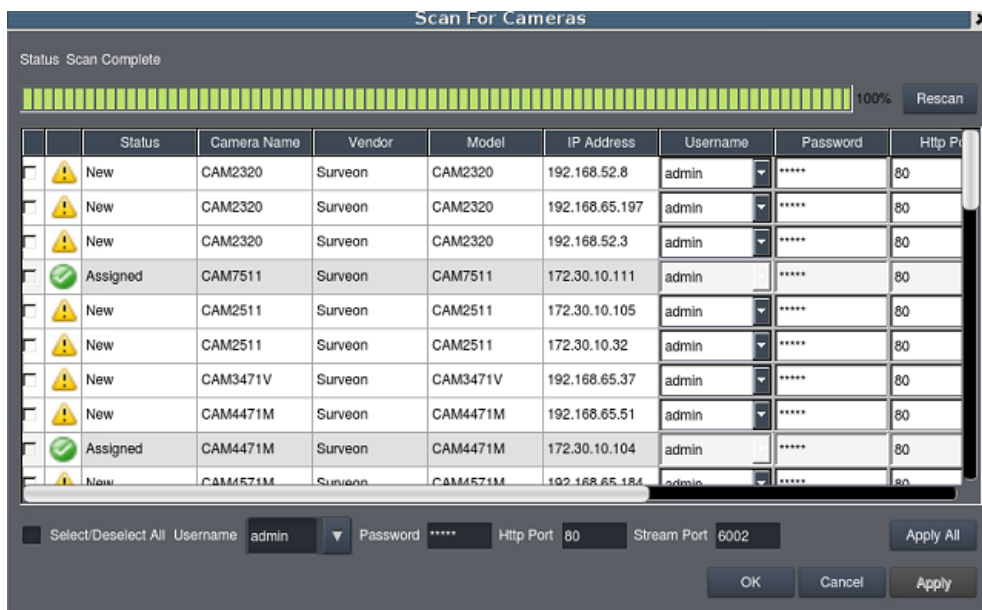
Cameras can be added to the Server in two ways: via an automatic scan or by manually inputting the camera information.

5.2.1. Automatic Scan for Cameras

Right-click on the camera to bring out the setting menu and select **Scan for Cameras**.



1. The system will respond by beginning an automatic scan. Once the scan is complete, the cameras that can be added to the Server will be displayed. Information available for each camera will include:

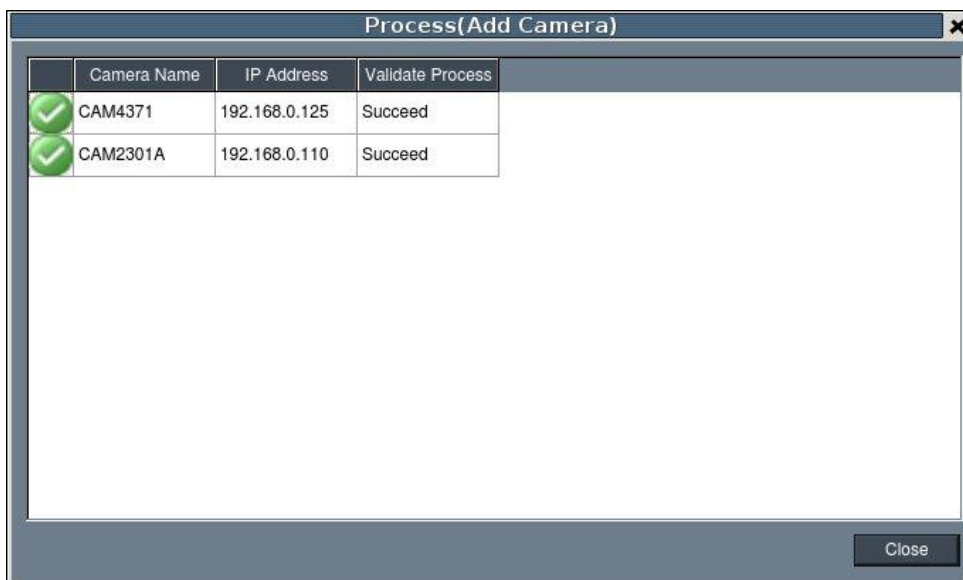


- **Name** - The default camera name (Make/Model)
- **Status** - The camera will display *New* if it has not been added to this Server, otherwise it will display *Assigned*.
- **IP Address**
- **MAC Address**
- **Vendor** - Including ACTI, Afreedy, AXIS, Arecont, BOSCH, Dahua, Dynacolor, EDIMAX, EverFocus, HIKVISION, IQinvision, JVC, LG, Panasonic, Surveon, and ONVIF.
- **Model**

2. To add a camera to the system, check the box by the camera entry. You may also check the **Select All** box at the bottom of the window to select all the cameras found.

Enter the username and password, and press **Apply Selected**. Click **OK** to add the selected cameras to the Server.

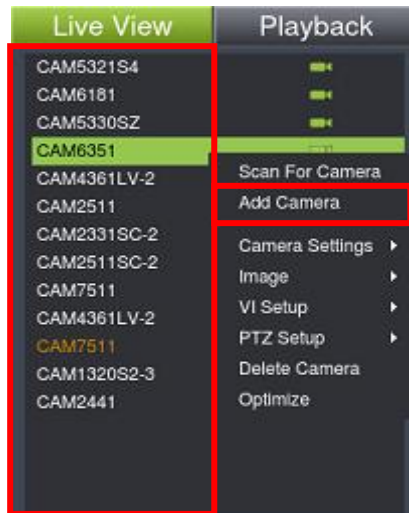
The following windows will prompt for validation.



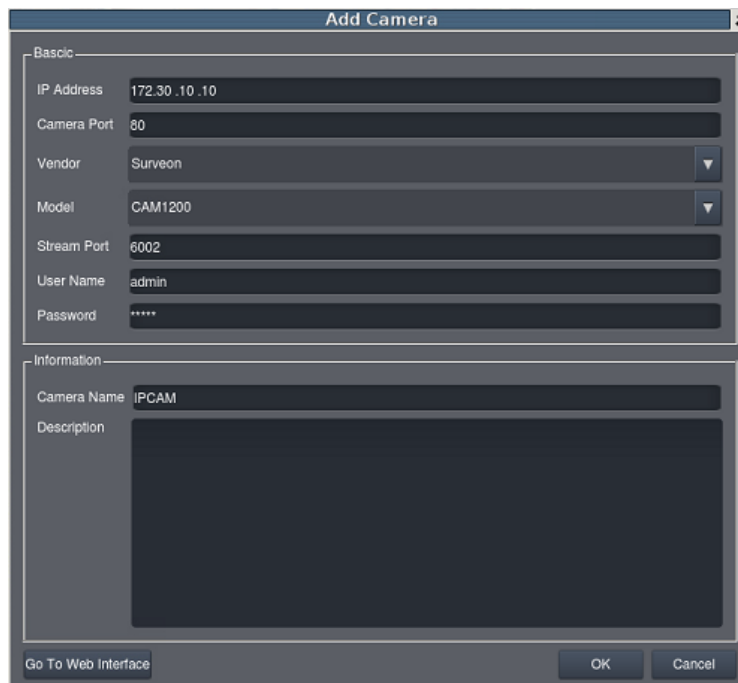
5.2.2. Manually Adding Cameras

To manually add a camera to the Server:

Right-click on the camera to bring out the setting menu and select **Add Camera**.



2. In the camera window fill out the following information:




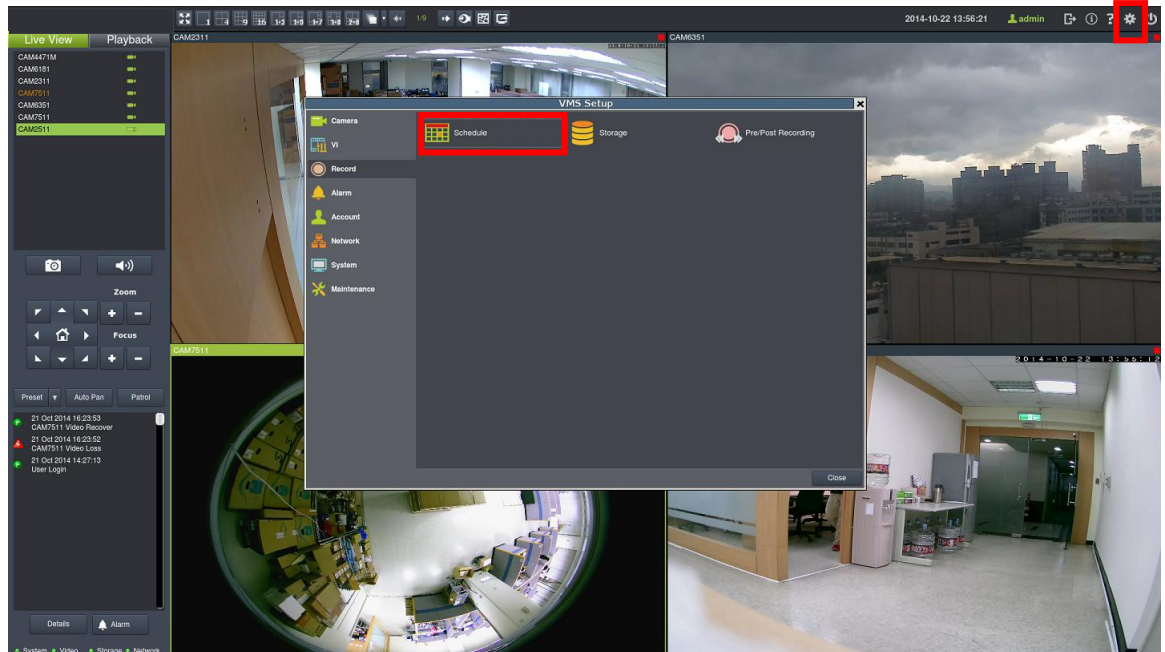
- **IP Address**
- **Camera Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **Vendor** - Including Including ACTI, Afreedy, AXIS, Arecont, BOSCH, Dahua, Dynacolor, EDIMAX, EverFocus, HIKVISION, IQinvision, JVC, LG, Panasonic, Surveon, and ONVIF.

- **Stream Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **User Name** - This value is not always required.
- **Password** - This value is not always required.
- **Camera Name** - It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**

5.3. Setting Recording Schedule

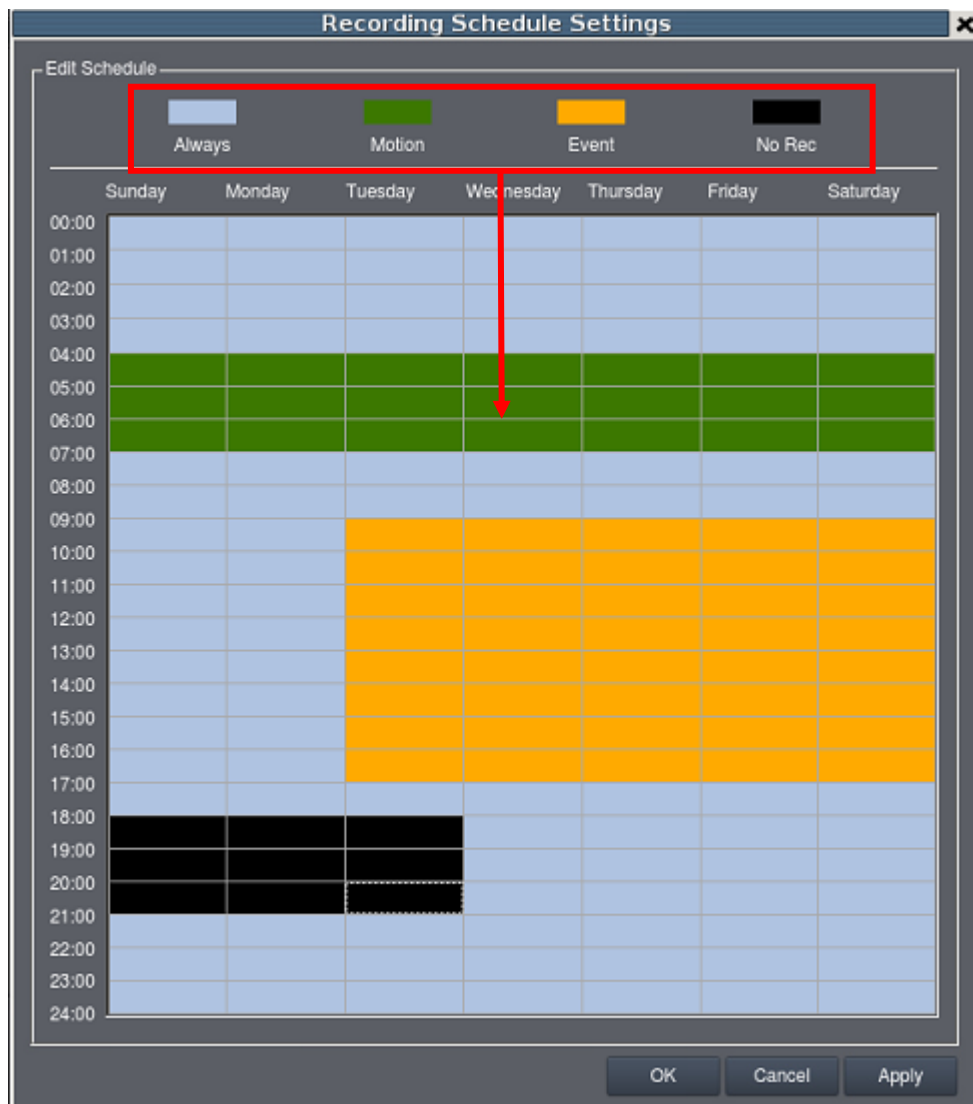
5.3.1. Recording Schedule

Click  to bring out **VMS Setup** window and select **Recording** and then **Recording Schedule**.



1. The schedule grid corresponds to every hour in the week. Click on one of the 4 recording methods and then click on the grid area to “paint in” the method for the corresponding hour.

2. Click the **Apply** button to apply the schedule and **OK** to exit the dialog.

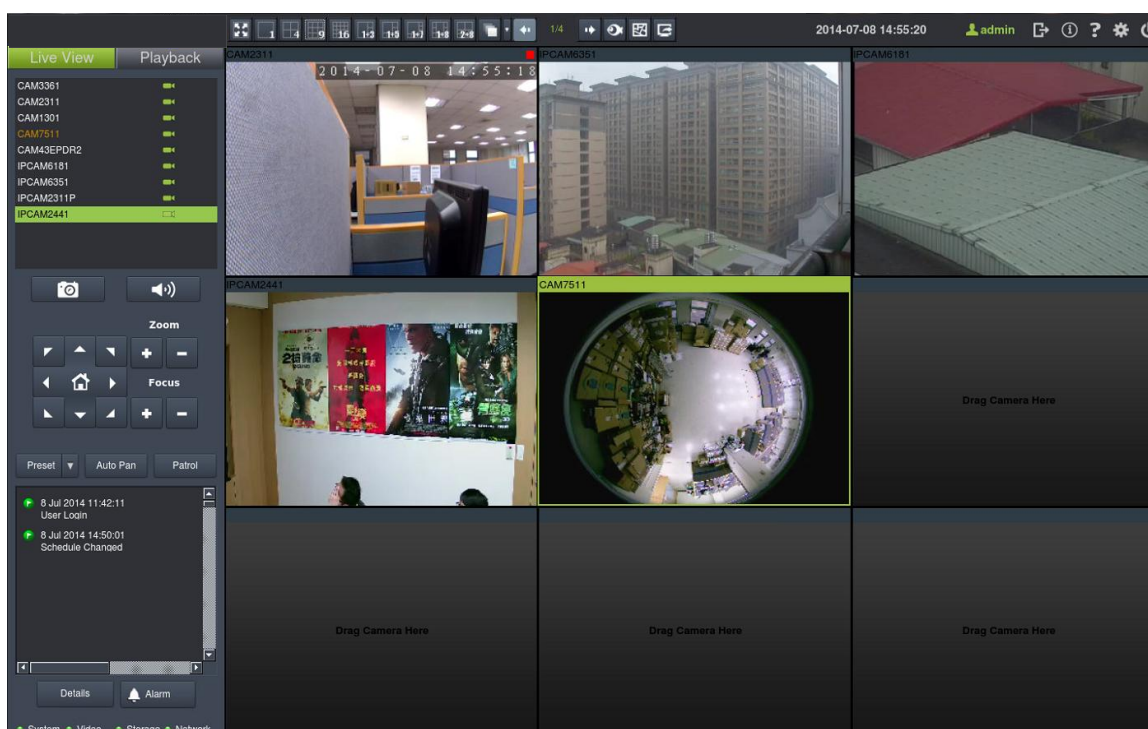


5.4. Setting up Live View

An important part of monitoring your surveillance network is to have the right views so that you will have the optimum viewing angle to discern a situation.

The default view setting is 4x4.

From the *Camera List*, you can click and drag each camera into separate frames. The camera output will be displayed in the frame.



Chapter 6 Live View

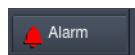
Live viewing is a crucial part of any surveillance system. Having the right view can be the crucial difference between catching an event as it happens and missing it altogether. VMS provides powerful tools to manage the viewing experience to help ensure that monitoring personnel are always on top of any event.

6.1. Live View Window Overview






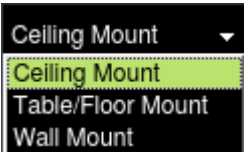






The live view window is split into 10 distinct parts:



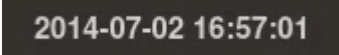
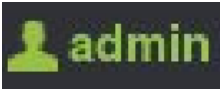







1. **Live View / Playback Selection Tabs** - Allows users to choose live view and playback mode.
2. **Camera List** - Lists all the connected cameras.
3. **Snapshot** - Take a snapshot of the current camera image.
4. **Volume Control** - Control the volume.
5. **Live View Control** - Interface for interacting with PTZ-enabled cameras.
6. **Log** - This area contains system, video, storage, network status information.
7. **Alarm** - When triggered, the icon will flick with a red colored alarm



8. **Details** - List all the detailed logs for review, query and export.
9. **Button Area** - This area contains the buttons to change views, enter the full screen mode, go to the next/previous page, go home and auto page flip between pages.

	Full screen mode
	Viewing screen modes
	Auto page flip between pages
	When there are more than 1 live view page, click these buttons to go to the next / previous page.
	Select this icon to have better views for fisheye camera
	Select according to the way your fisheye is installed to have a best viewing result, Ceiling Mount, Table/Floor Mount or Wall Mount.
	<p>The distorted hemispherical image of the fisheye camera can be converted into a conventional rectilinear projection , a split-window , a 4 split-window , with 3 enlarge windows and 1 original image window, , an enlarged window and the original fisheye view .</p>

	E-map
	Send to the Secondary Display
	Date and time
	Signed in User Account
	Logout
	About contains version and product information
	Enclosed with the user manual
	Setup button
	Shutdown button

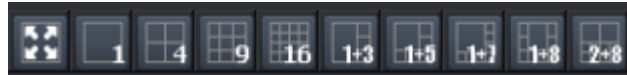
10. Main View Area - This area contains the actual video feed(s).

6.2. View Setup

6.2.1. Switching Between Different Screen Divisions

Creating and Using New Screen Divisions


When a view is created, it has a default screen division setting, however when using the view, it may be useful to change the number of screen divisions. This does not create a different view, but divides the existing view into a new set of divisions.



To perform this function within the view, simply click the button corresponding to the view that you want to use. The buttons are located in the area above the main view window.

After you have clicked on the desired view, the cameras will be divided into separate pages in the selected view; the formula is $36/\text{selected view number}$. For example, a one view will have a 36 pages of views and a 1+5 view will be $36/6$, 6 pages of views.

Auto-flipping Pages

When multiple pages of screen divisions exist, you may choose to automatically flip between the pages by clicking on the  button. Clicking the button again will end the automatic flip function.



Screen Division Page Use

The page number is displayed to the right of the view buttons. Clicking on the arrow button to the right of the page number or clicking on the current screen partition button will scroll through the pages in order. Clicking on the arrow button to the left of the page number will scroll through the pages in reverse order.







Fisheye View

Click the **Fisheye** button in the button area when using a fisheye camera. This will bring out a selection of views for fisheye camera to have better view results.



Select according to the way your fisheye is installed to have a best viewing result, Ceiling Mount, Table/Floor Mount or Wall Mount.

Icon	Description	Reference
	conventional rectilinear projection, panorama view	
	split-window, horizontal view	
	4 split-windows: 3 enlarged view windows and 1 original fisheye window. Place the different colored boxes in the original fisheye window on the upper right corner to have detailed views projected on the other viewing windows.	

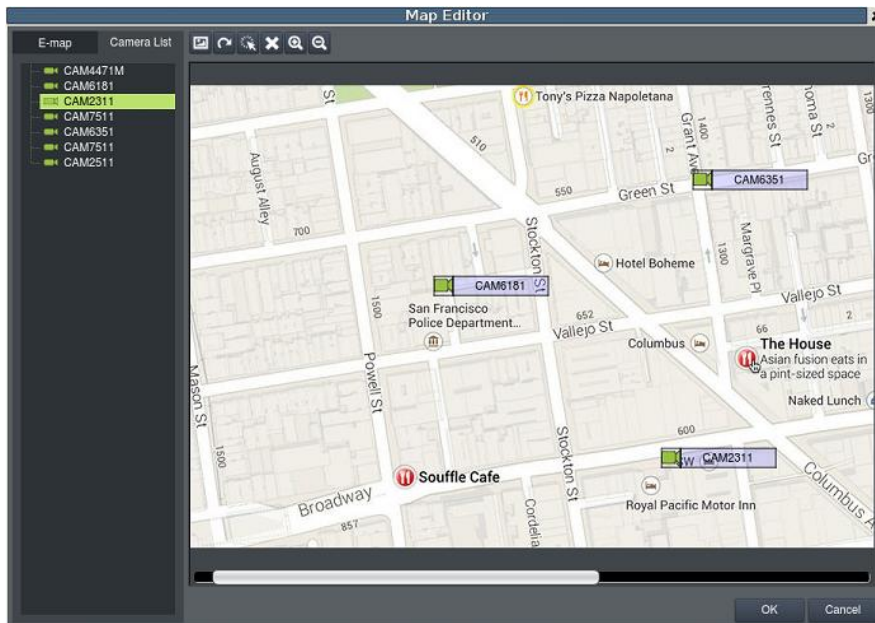
	<p>1 enlarged view window and 1 an original fisheye window.</p> <p>Place the colored box in the original fisheye window on the upper right corner to have a detailed view projected.</p>	
	<p>original fisheye view</p>	

E-map

Click the **E-map** button in the button area to open an existing E-map or create an E-map.

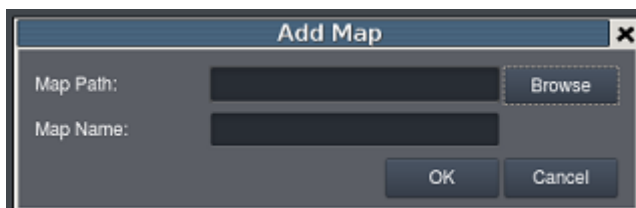
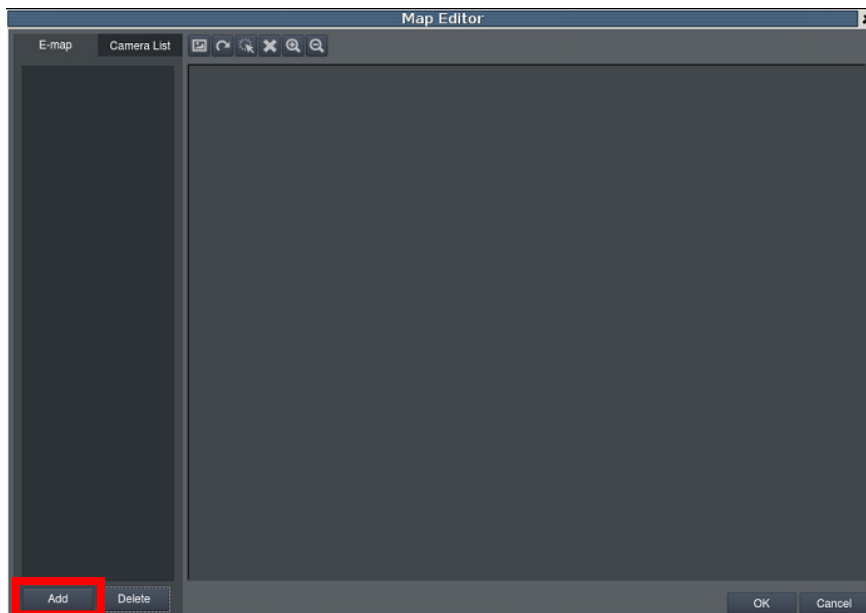


When there is an existing E-map, the E-map will be shown as below. You can click the set camera on the map to see its surroundings. If there is an alarm, the set camera on the E-map will begin flicking and you can have a better idea where the event took place.

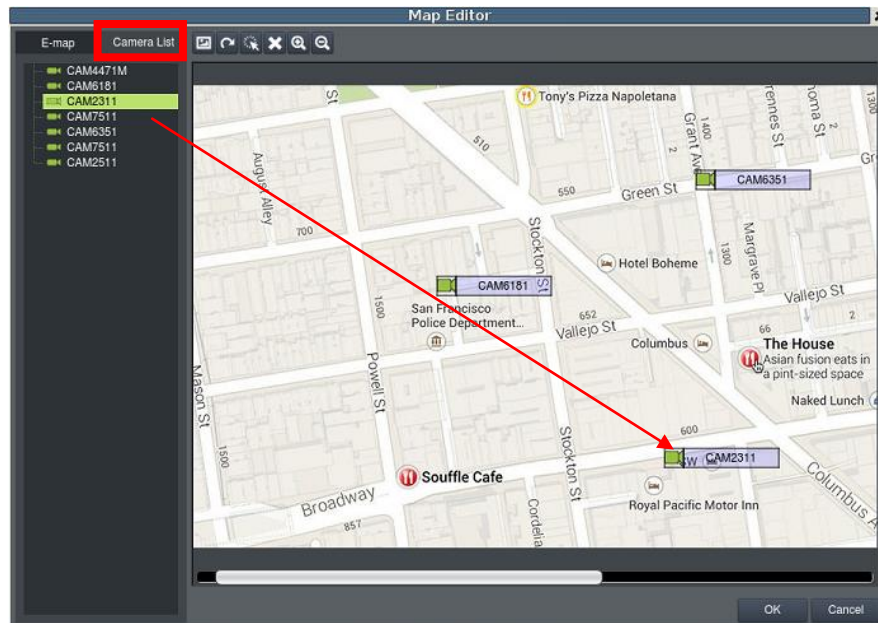



When there is no E-map stored, the system will ask you to add an E-map. Follow the steps below to create an E-map.

1. Prepare layout drawings or a map of the area being surveyed.
2. Click the **Add** button to bring out the **Add Map** window.



3. Click the **Browse** button to open a windows dialog. Select your map and click the **Open** button. The drawing will be stored in the Server.
4. Enter a name for the map in the **Map Name** field.
5. Click **Save**. Once successfully added, an E-map node will appear.
6. Go to the Camera List tab to drag and drop the cameras to the desired location on the E-map to complete the E-map creation.



For camera relocation, click  to select the cameras and then the selected camera can be moved.

Go to **VMS Setup > System > Map Editor** in the setup to add another E-map or any further setups.

Secondary Display

Click the **Secondary Display** button in the button area when you have the second monitor, the view will be sent to the secondary display.

6.3. Functionality Within Views

Right clicking an active window will cause a function list to appear. These are settings and functions that can be changed within the live-view window.



6.3.1. Digital Zoom

Digital zoom increases the view size without increasing resolution. The digital zoom function can be used within any panel (even in full screen mode) with the following steps:

1. Right-click the panel that zoom is required on, and select **Digital Zoom** to activate the function. A picture-in-picture showing the whole screen framed by a yellow box will appear.
2. Use the mouse scroll to zoom into the center of the image. Scrolling forward will zoom in, scrolling backward will zoom out. Click the corners of the box and drag to the area of interest. The main picture will show the digitally-zoomed output, while the picture-in-picture will display the entire view.



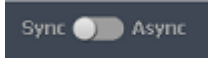


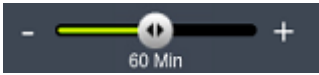





6.3.2. Instant Playback











The instant playback function gives users the ability to instantly playback up to 45 minutes of video. Right-click the video panel that playback is required on, and select **Instant Play > [Time Length]** to activate the function. A popup will open with the desired playback. Time lengths available are dependent on, and will not exceed the pre-alarm recording time set in [Pre/Post Recording](#).





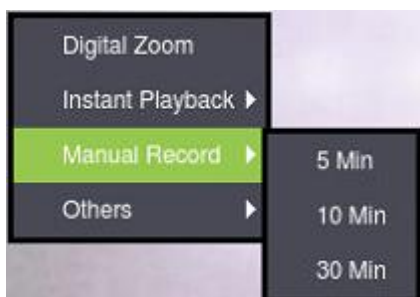
The following table explains the buttons:

	Sync all the views to play videos from the same period of time. While in the Sync mode, the view cannot be changed. Async, undo syn, different views can be selected.
	Snapshot
	Audio volume
	Time range can be set when viewing the playback.
	Full frame mode
	Key frame mode
	Saves video clips/Exports selected clips
	Clear all the Cue-Ins and Cue-Outs
	Set Cue-In marker for clip start

	Set Cue-In marker for clip end
	Automatic reply the clip. (From Cue-in to Cue-Out)
	Starts video playback
	Pause video playback
	Stops video playback.
	Jumps to the previous frame
	Jumps to the next frame
	Jumps to the previous segment
	Jumps to the next segment
	The play speed can be adjusted from 1x to 8x.

6.3.3. Manual Recording

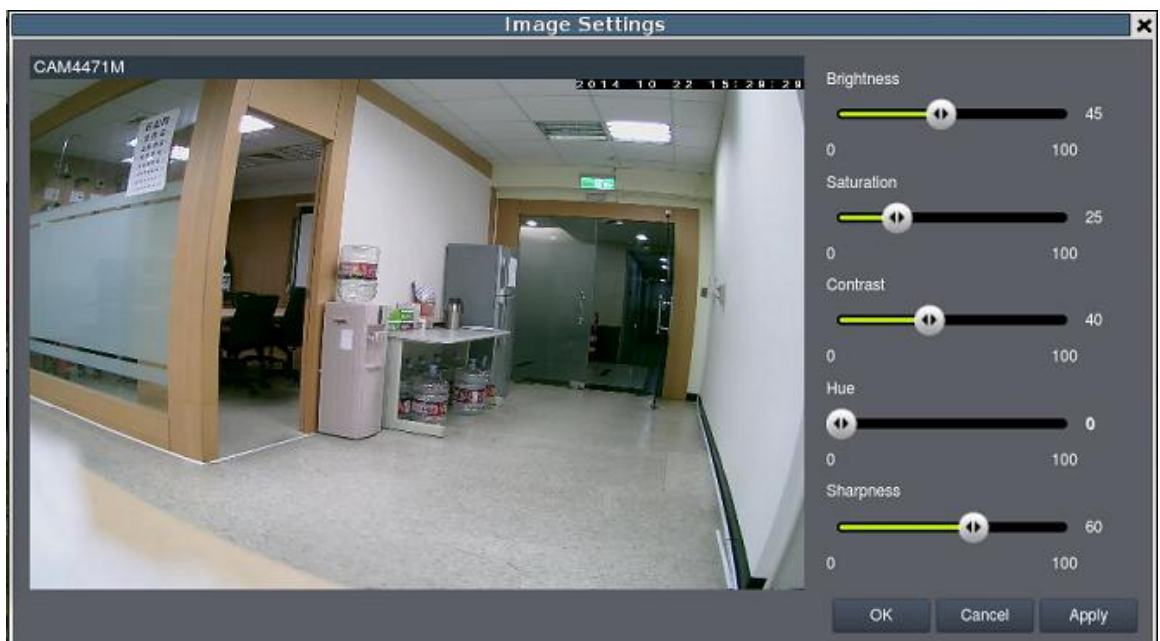
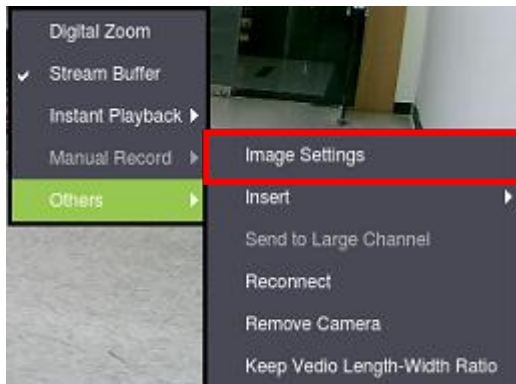
When recording schedules are set, it may be necessary to manually record a video stream, even when the schedule does not specify for recording. In this case right-click the panel that recording is required on, and select **Manual Record > [5, 10 or 30 minutes]** to activate the function. The camera will record the stream for the amount of time specified.



6.3.4. Others

Image Settings

Camera image settings can also be accessed by right-clicking the panel containing the camera video and selecting **Others > Image Settings**.



1. Adjust the following sliders to change the camera image:

- **Brightness** - The overall lighting level of the image. This value can be used to boost or reduce the apparent lighting of the image.
- **Saturation** - The overall color intensity of the image. This value can be used to boost or reduce overall color intensity.
- **Contrast** - The lighting difference between dark and light areas of the image. This value can be used to boost or reduce apparent differences in lighting.

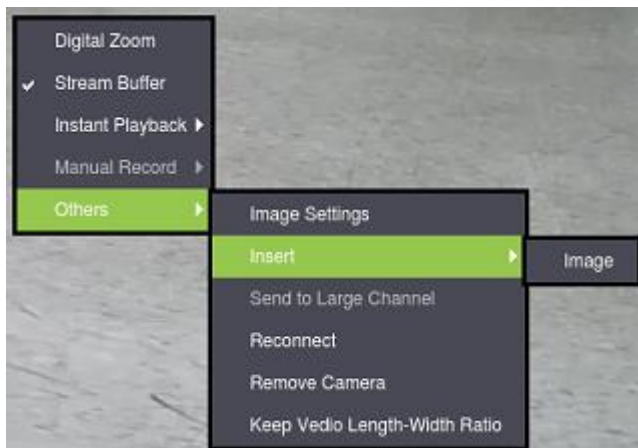
- **Hue** - The color cast of the image. This value can be used to compensate for colored lighting or other color casting.
- **Sharpness** - The edge contrast of the image. This value can be used to make the picture appear clearer.

2. Click **OK** to save your changes.

Note: Camera Image Settings can also be configured by right-click the camera entry in the *Camera List below the Live View*, then click **Image Adjustments > Image Settings**.

Insert

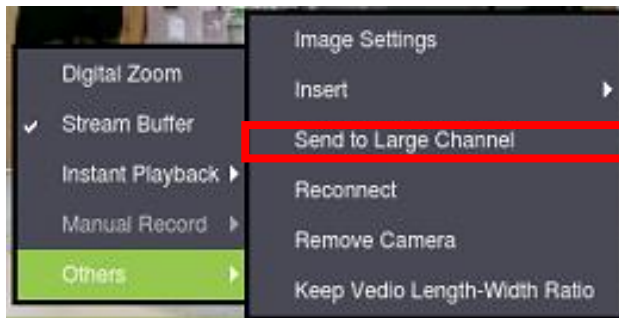
The panel can be replaced with a user overlay.



To overlay an image on top of a panel:

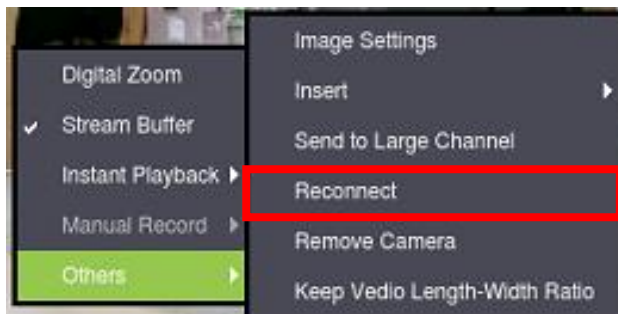
1. Right-click the panel and choose **Others > Insert > Image**. The system will prompt you to choose an image file.
2. Choose an image file, valid image types are JPEG, BMP, TIF, PNG. Click **Open** to open the file.
3. The image will be displayed in the panel. Click the red X in the top-right corner to close the image.

Send to Large Channel



When the view with different sizes is selected, views in smaller divisions can be switched to the larger division. To perform this action, right-click the panel corresponding to the camera and choose **Others > Send to Large Channel**.

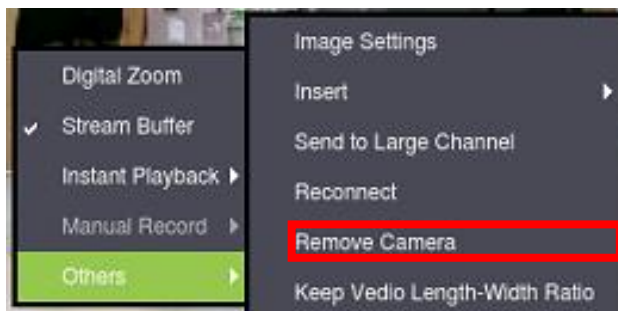
Reconnect



In some cases it may be necessary to manually reset the connection to a camera. To perform this action, right-click the panel corresponding to the camera and choose **Others > Reconnect**.

Remove the Camera

The Cameras can be removed by clicking **Others > Remove Camera**.



6.4. Full Screen View

6.4.1. Entering Full Screen View

From any view, you can switch to full screen mode by clicking on the full screen button located above the main viewing window. Optionally you may also choose to view a single frame in full screen mode by double clicking on the frame.



6.4.2. Exiting Full Screen Mode

To exit full screen mode, hit the **ESC** key on your keyboard.


Chapter 7. Server Setup

This section deals with Server setup procedures.

7.1. Server Settings

7.1.1. General Server Settings

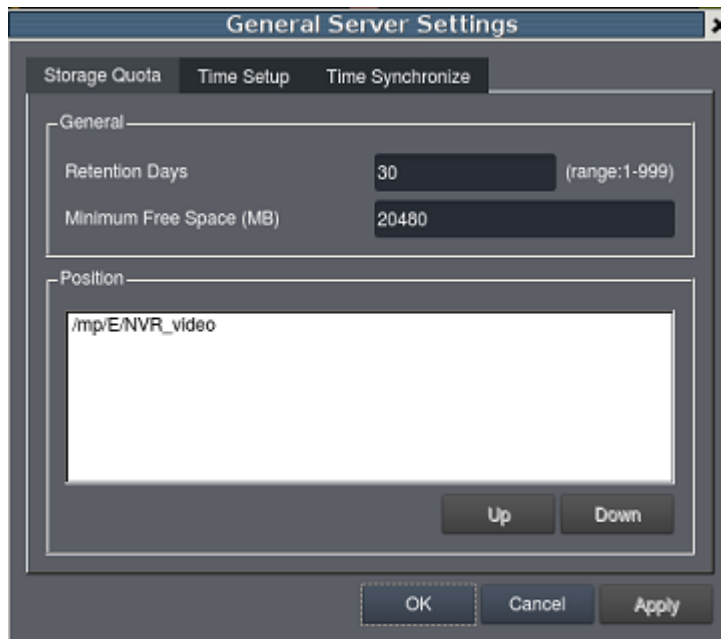
The following sections deal with Server settings that can be configured under the *Server Settings* menu.

1. Click  to bring out **VMS Setup** window and select **System** and then select **General Server Settings**.



2. A tabbed window will appear providing the following configuration tabs: *Storage Quota and Time Settings*.

■ Storage Quota

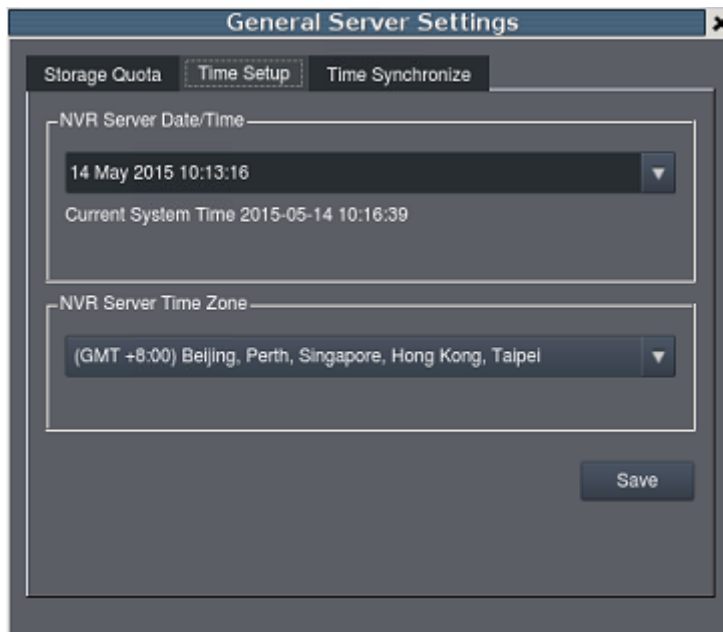


The image shows the 'General Server Settings' dialog box with the 'Storage Quota' tab selected. The 'General' section contains two fields: 'Retention Days' set to 30 (with a range of 1-999) and 'Minimum Free Space (MB)' set to 20480. The 'Position' section contains a list box with the path '/mp/E/NVR_video' and 'Up' and 'Down' buttons. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Section	Field	Value	Notes
General	Retention Days	30	(range:1-999)
	Minimum Free Space (MB)	20480	
Position	Path	/mp/E/NVR_video	
	Buttons	Up, Down	Change storage priorities

In the **Minimum Free Space** field, the Minimum space required for storage is shown. The storage will be last for 30 days. Click on the items in the Position section and use the **Up** and **Down** buttons to change the storage priorities.

■ Time Setup

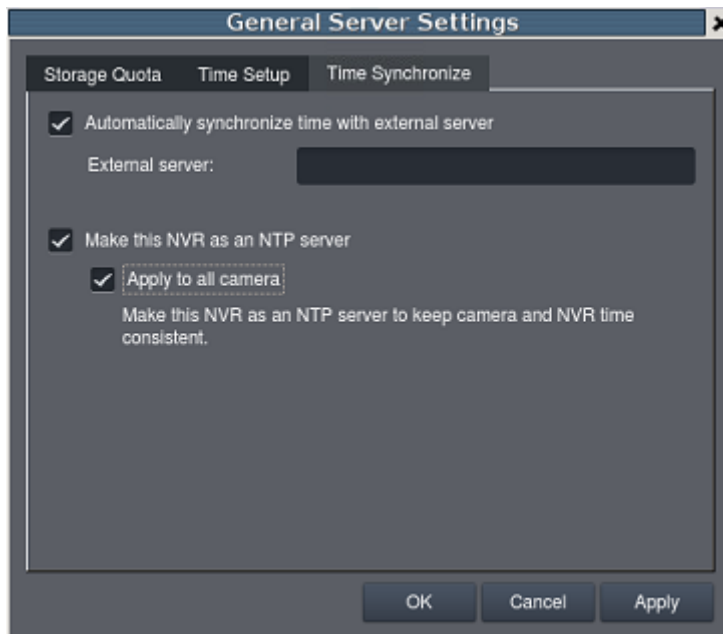


The image shows the 'General Server Settings' dialog box with the 'Time Setup' tab selected. The 'NVR Server Date/Time' section shows a dropdown menu with '14 May 2015 10:13:16' and the 'Current System Time 2015-05-14 10:16:39'. The 'NVR Server Time Zone' section shows a dropdown menu with '(GMT +8:00) Beijing, Perth, Singapore, Hong Kong, Taipei'. A 'Save' button is at the bottom right.

Section	Field	Value
NVR Server Date/Time	Date/Time	14 May 2015 10:13:16
	Current System Time	2015-05-14 10:16:39
NVR Server Time Zone	Time Zone	(GMT +8:00) Beijing, Perth, Singapore, Hong Kong, Taipei

To set the server time click on the number you wish to change and enter a value. Click **OK** to preserve the setting. The default time is set according to the real-time clock on server.

■ Time Synchronize




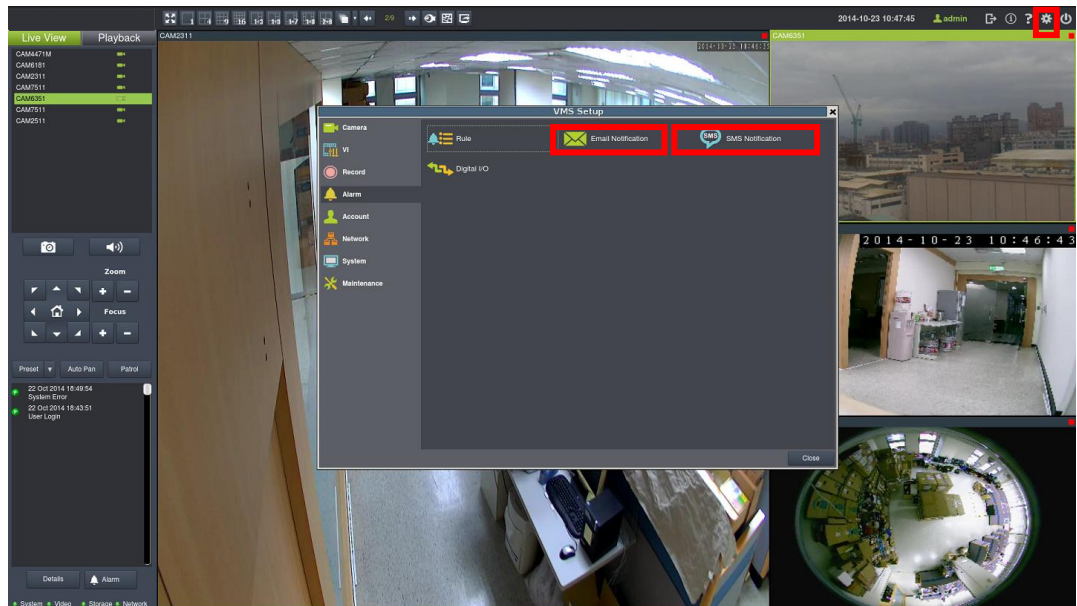
To synchronize the system time with the external server, check the option "Automatically synchronize time with external server" to enable this functionality. And input the IP address of the external server in the External Server field.

Check the option "Make this NVR as an NTP server" to enable this functionality.

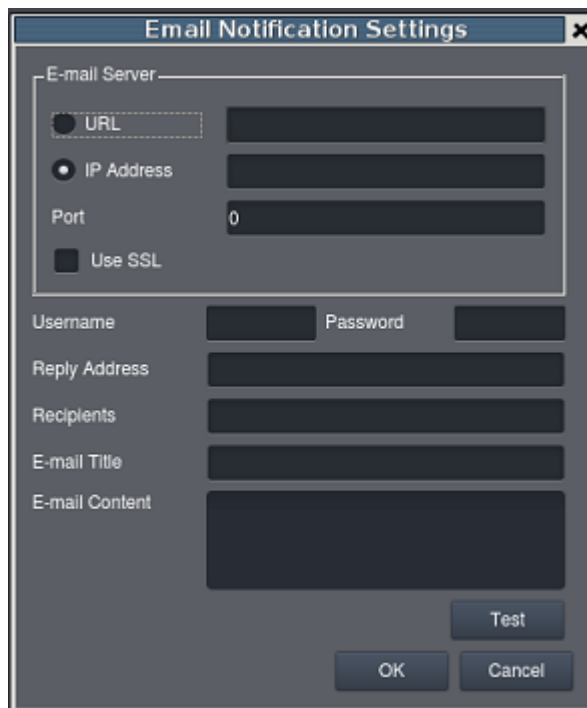
And check the option "Apply to all camera" to make this SMR as an NTP server and to have camera time and SMR time synchronized.

7.1.2. To perform Notification Setting

1. Click  to bring out VMS Setup window and select **Alarm** and then select **Email Notification** or **SMS Notification**.



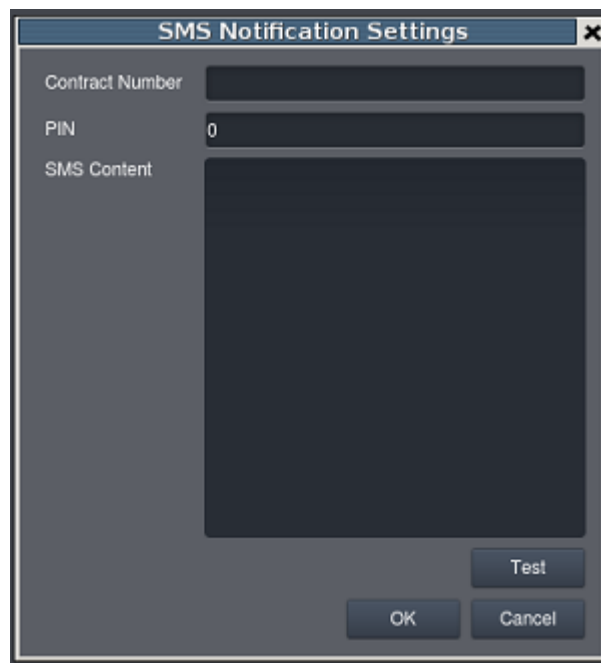
2. Click **Email Notification** tab to continue.

The 'Email Notification Settings' dialog box is shown. It has a tab for 'E-mail Server'. Under this tab, there are fields for 'URL', 'IP Address', 'Port', and 'Use SSL'. Below these are fields for 'Username', 'Password', 'Reply Address', 'Recipients', 'E-mail Title', and 'E-mail Content'. There are 'Test', 'OK', and 'Cancel' buttons at the bottom.

- 2.1. You may either enter the URL (such as smtp.abc.com) or IP address of the SMTP server that the Server will use to deliver E-mail notifications. The SMTP server configured here must support Unicode Transformation Format-8 (UTF-8) encoding.

- 2.2. Enter the user name for the Server email account in the **Username** field.
- 2.3. Enter the password for the Server email account in the **Password** field.
- 2.4. Enter a valid E-mail address in the **Reply Address** field. This address will be the default sender listed in E-mails sent from the Server.
- 2.5. Enter one or more E-mail addresses in the **Recipients:** field. These address(es) will receive notifications from the Server. Multiple addresses can be entered by separating individual addresses with semi -colons “;”.
- 2.6. Enter the subject of your notification E-mails, e.g., Server-xxxxsite1notification in the **E- Mail Title** field.
- 2.7. Enter a short message in the large field to describe the Server or a surveillance network.
- 2.8. (Optional) Click **Test** to send a test message to the E-mail addresses listed.

3. Click the **SMS Notification** to continue.

The image shows a software dialog box titled "SMS Notification Settings" with a close button (X) in the top right corner. Inside the dialog, there are three input fields: "Contract Number" (empty), "PIN" (containing the digit "0"), and "SMS Content" (a large empty text area). At the bottom right of the dialog, there are three buttons: "Test", "OK", and "Cancel".

- 3.1. In the **Contact Number** field, enter the phone numbers that will receive SMS notifications. Be sure to include the area code, e.g., “86”, in front of phone numbers. Use commas, “,” to separate individual phone numbers.
- 3.2. Use the slider bar to select a delay between the occurrence of an event and SMS message delivery.

3.3. **(Optional)** If a SIM PIN is required, enter the PIN code in the **PIN** field. Note that applying incorrect PIN code may disable your SIM card.

Note: To change the PIN code, remove the SIM card from your GSM modem. Use a cell phone to change the PIN code and then re-install SIM card into the GSM modem. Changing PIN codes is not recommended because a configuration failure may disable your SIM card.


3.4. In the **SMS Content** field, type a simple description to include in the outgoing SMS messages

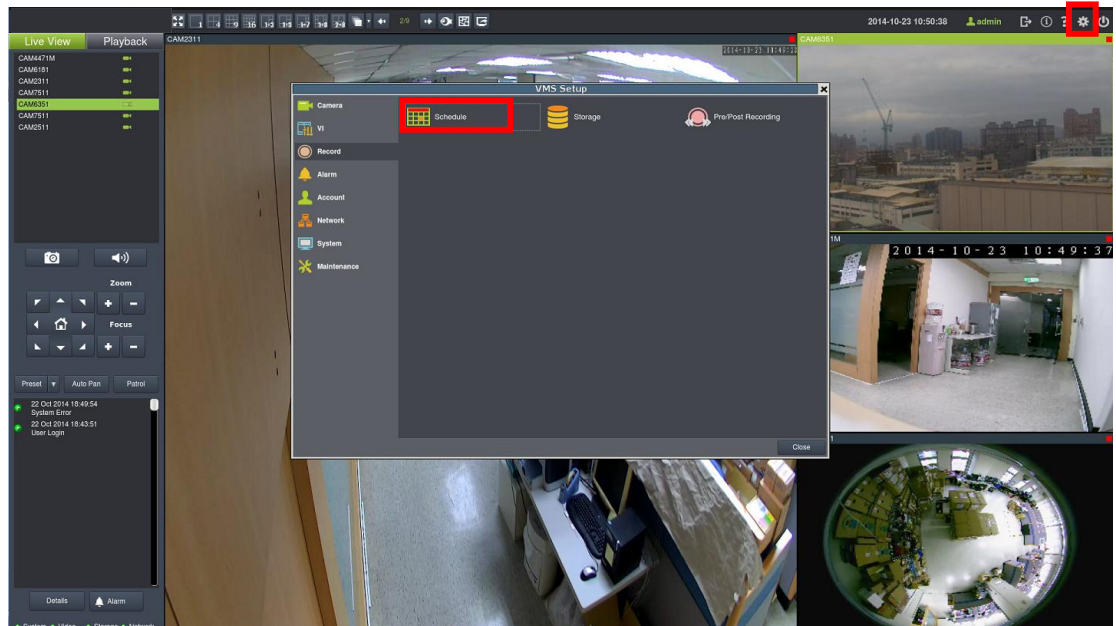
3.5. **(Optional)** Click **Test** to send a test message to the phone numbers listed.

3.6. Click the **Apply** button to apply the changes.

3.7. Click the **OK** button to exit E-mail/SMS settings.

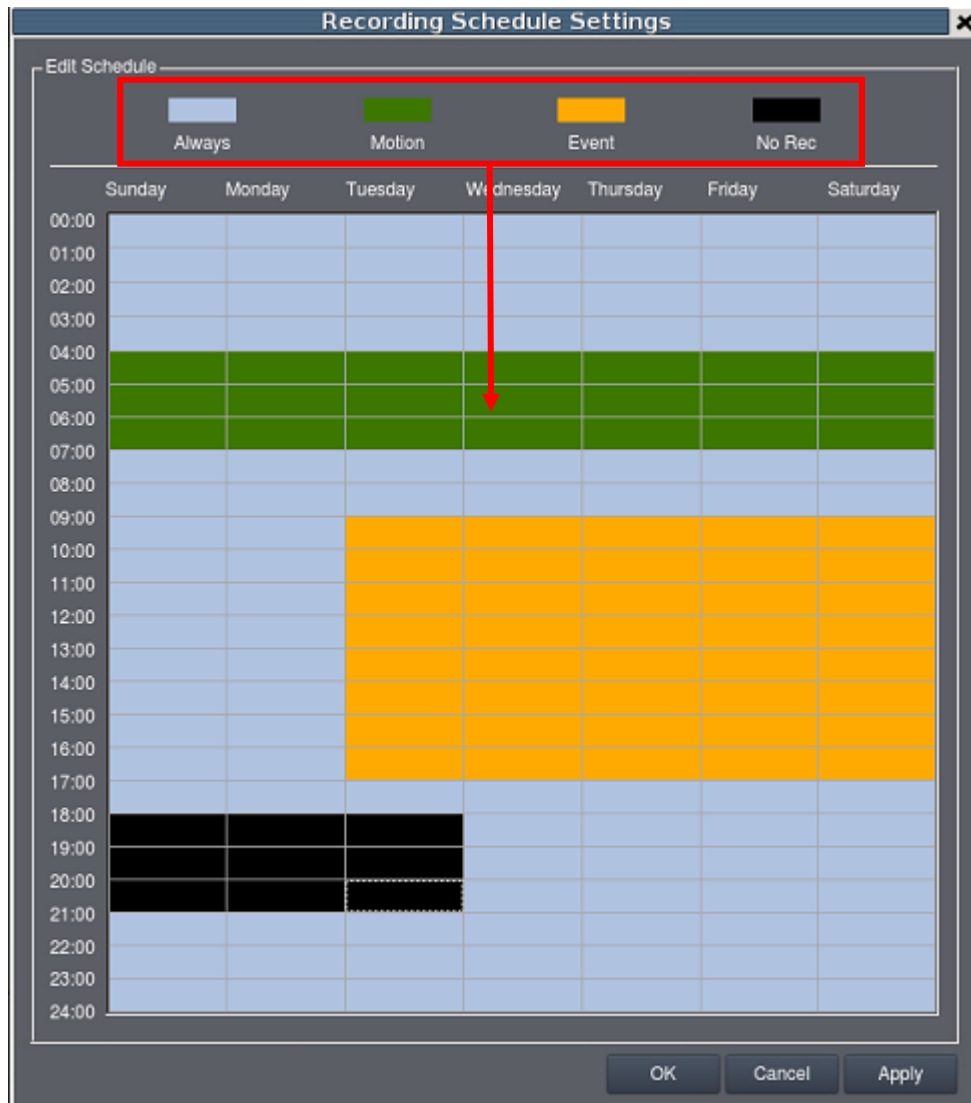
7.1.3. Scheduling Recording

Click  to bring out VMS Setup window and select **Recording** and then **Recording Schedule**.




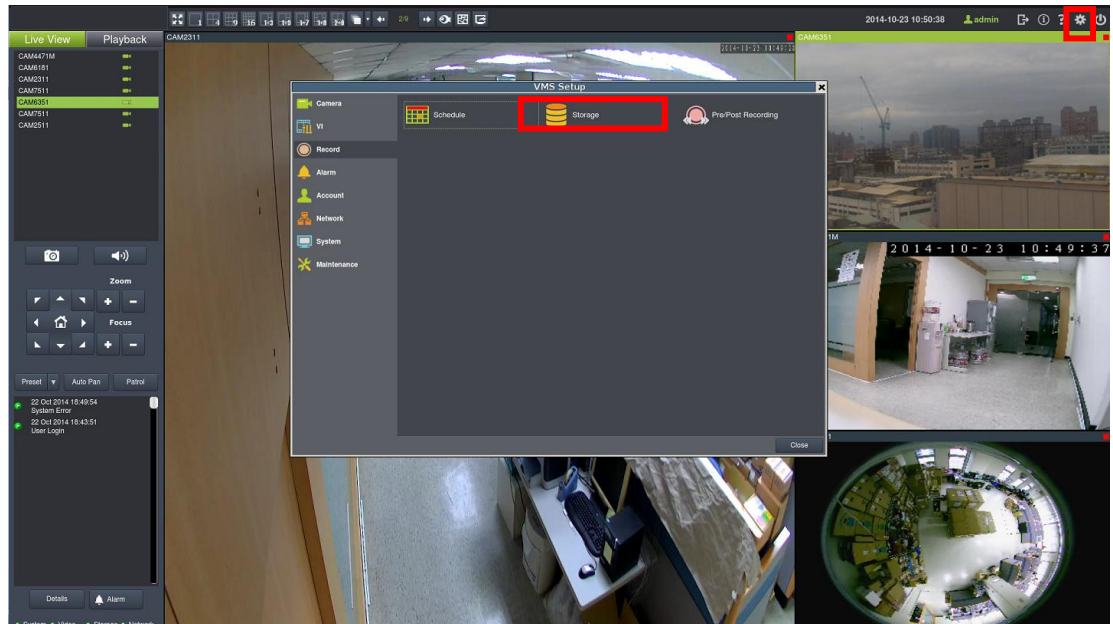
The schedule grid corresponds to every hour in the week. Click on one of the 2 recording methods and then click on the grid area to “paint in” the method for the corresponding hour.

1. Click **OK** to save the settings and exit the dialog.

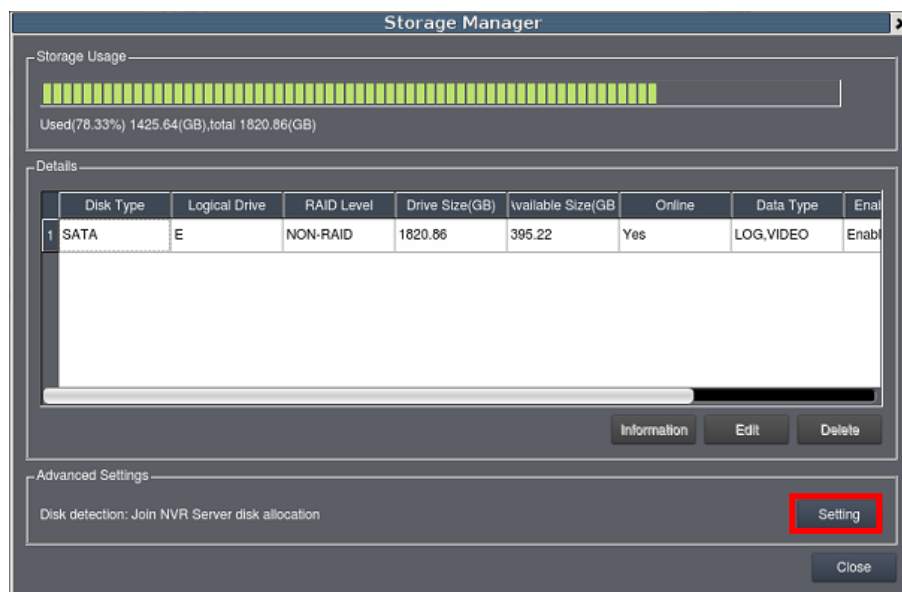


7.1.4. Storage Management

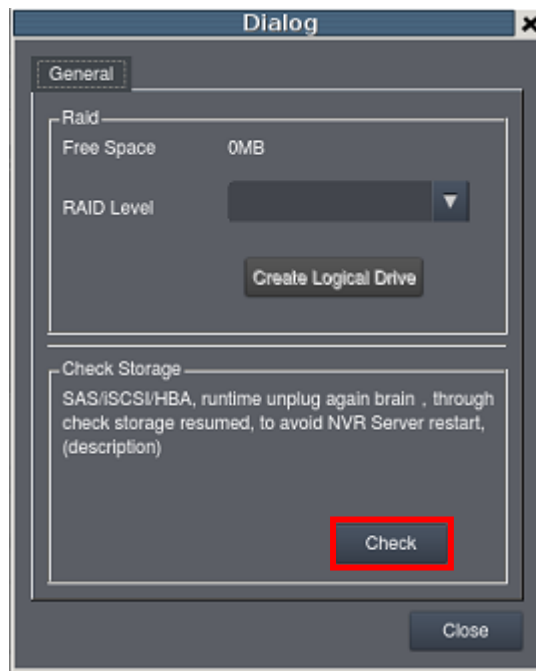
1. To access the information about the drives configured in your Server, click  to bring out **VMS Setup** window and then select **Recording** to see and click **Storage** option for **Storage Manager**.



2. All available Logical Drives, as well as their sizes, free space, and status will appear. Click target drive and then **Setting** to set the log and location for saving the video recordings.




3. Click the target drive first and then **Settings**. In “General” tab, click **Check**.

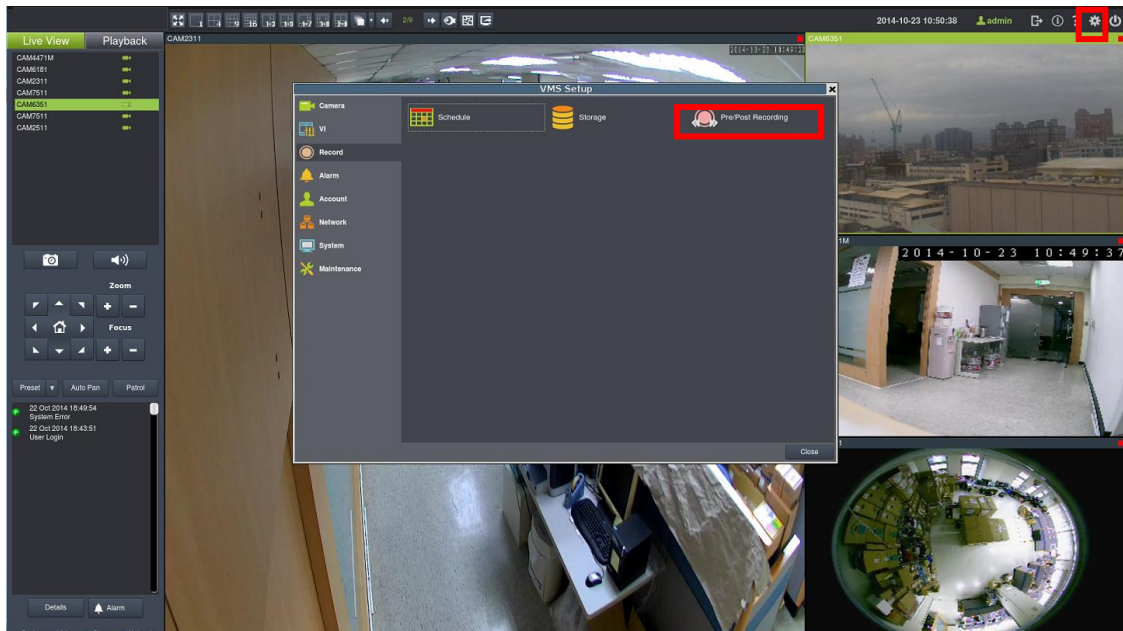


4. Choose the RAID level, and then click **Create Logical Drive** to create the RAID configuration.

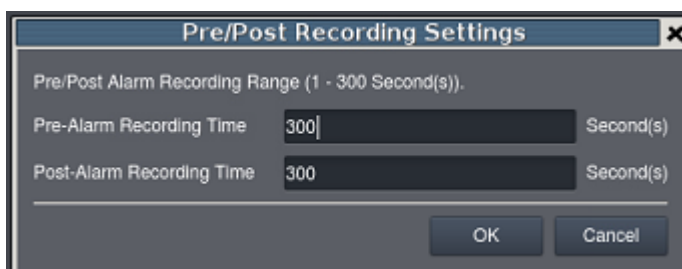
7.1.5. Pre/Post Recording

Video streams are constantly processed and cached in memory. The Server can trace back and preserve video/images from several minutes before and after the occurrence of an alarm.

Click  to bring out **VMS Setup** window and select **Recording** and then select **Pre/Post Recording**.



The following pop-up window will appear:



In each of the boxes enter values for the Pre and Post Recording times from 1 to 300 seconds (default is 300 seconds). Click the **OK** button to finish the process.

Chapter 8. Camera Setup

This section deals with Camera setup procedures. These options can be accessed by right-clicking the Camera entry in the *Camera List below the Live View*.

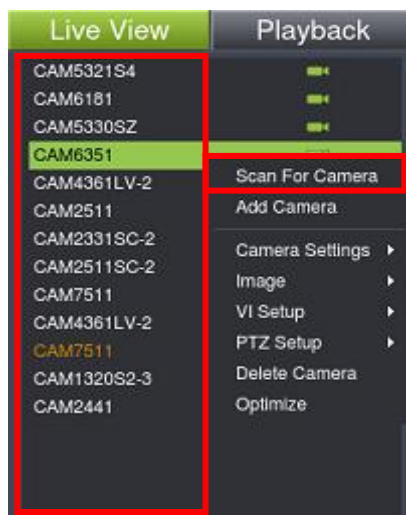
8.1. Adding Cameras

Cameras can be added to the Server in two ways: via an automatic scan or by manually inputting the camera information.

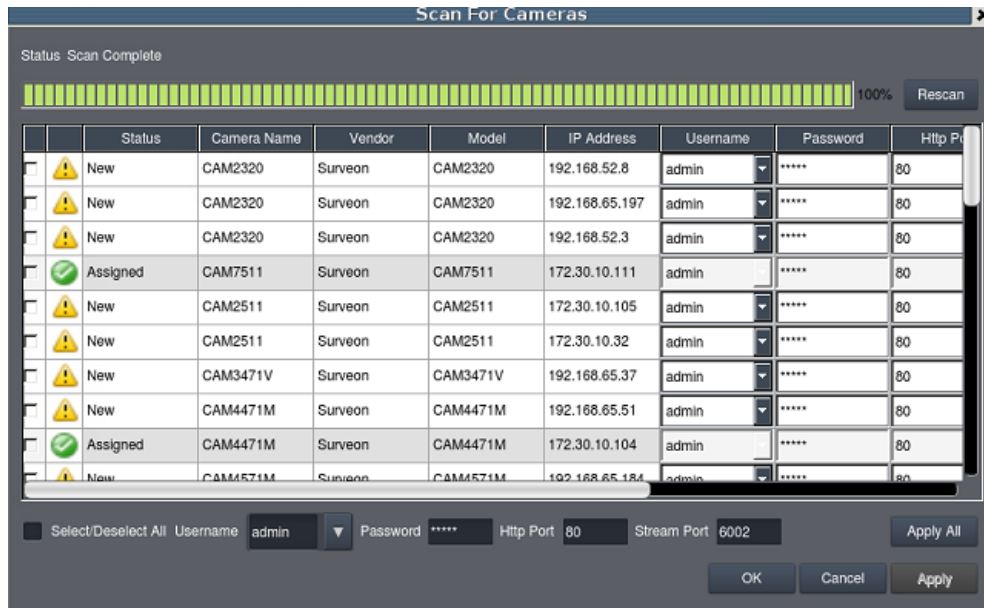
8.1.1. Automatic Scan for Cameras

To begin an automatic scan for cameras:

Right-click on the camera to bring out the setting menu and select **Scan for Cameras**.



1. The system will respond by beginning an automatic scan. Once the scan is complete, the cameras that can be added to the Server will be displayed. Information available for each camera will include:

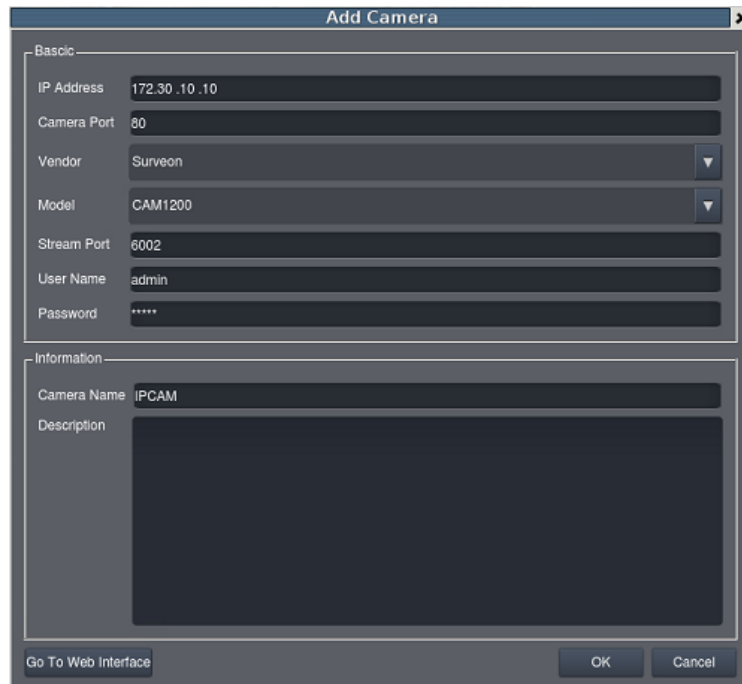


- **Status** - The camera will display *New* if it has not been added to this Server, otherwise it will display *Assigned*.
- **Camera Name** - The default camera name (Make/Model)
- **Vendor** - Including ACTI, Afreey, AXIS, Arecont, BOSCH, Dahua, Dynacolor, EDIMAX, EverFocus, HIKVISION, IQinvision, JVC, LG, Panasonic, Surveon, and ONVIF.
- **Model**
- **IP Address**
- **Username**
- **Password**
- **Http Port**
- **Stream Port**
- **MAC Address**

2. To add a camera to the system, check the box by the camera entry. You may also check the **Select All** box at the bottom of the window to select all the cameras found.

Enter the username and password, and press **Apply Selected**. Click **OK** to add the selected cameras to the Server.

3. (Optional) Double-click any camera entry to bring up the camera detail page. From this page you may change the following information:



The screenshot shows a window titled "Add Camera" with a close button (X) in the top right corner. The window is divided into two main sections: "Basic" and "Information".

Basic Section:

- IP Address: 172.30.10.10
- Camera Port: 80
- Vendor: Surveon (dropdown menu)
- Model: CAM1200 (dropdown menu)
- Stream Port: 6002
- User Name: admin
- Password: *****

Information Section:

- Camera Name: IPCAM
- Description: (Large empty text area)

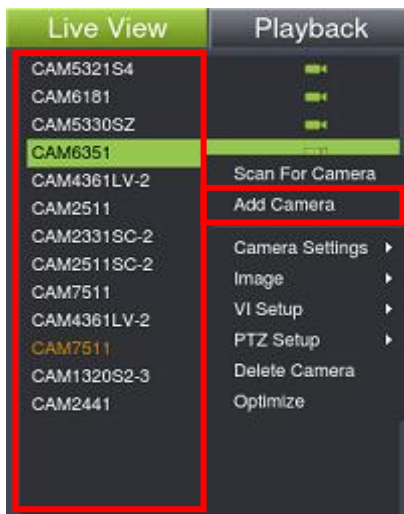
At the bottom of the window, there are three buttons: "Go To Web Interface", "OK", and "Cancel".

- **IP Address** - Changing this value will affect connectivity.
- **Camera Port** - The web access port, default is 80.
- **Vendor** - Changing this value will affect connectivity.
- **Model** - Changing this value will affect connectivity.
- **Stream Port** - Default is 6002.
- **User Name** - This value is not always required.
- **Password** - This value is not always required.
- **Information**
- **Camera Name** - It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**

8.1.2. Manually Adding Cameras

To manually add a camera to the Server:

Right-click on the camera to bring out the setting menu and select **Add Camera**.



2. In the camera window fill out the following information:

A screenshot of a dialog box titled 'Add Camera'. It has two main sections: 'Basic' and 'Information'. The 'Basic' section contains the following fields: IP Address (172.30.10.10), Camera Port (80), Vendor (Surveon), Model (CAM1200), Stream Port (6002), User Name (admin), and Password (masked with asterisks). The 'Information' section contains: Camera Name (IPCAM) and a large empty text area for Description. At the bottom, there are three buttons: 'Go To Web Interface', 'OK', and 'Cancel'.

- **IP Address** - Changing this value will affect connectivity.
- **Camera Port** - The web access port, default is 80.
- **Vendor** - Changing this value will affect connectivity.
- **Model** - Changing this value will affect connectivity.

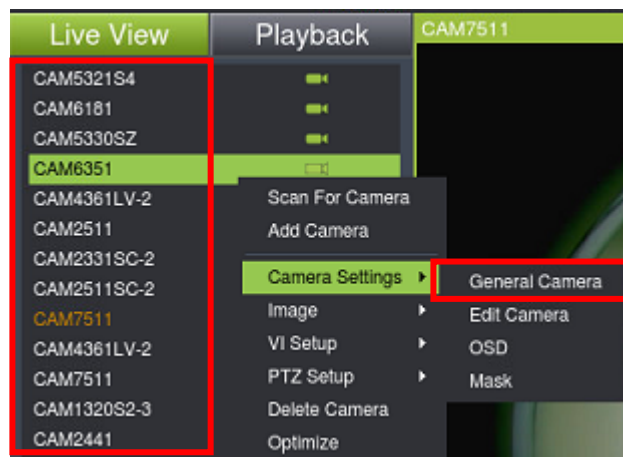
- **Stream Port** - Default is 6002.
- **User Name** - This value is not always required.
- **Password** - This value is not always required.
- **Information**
- **Camera Name** - It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**

8.2. Camera General Settings

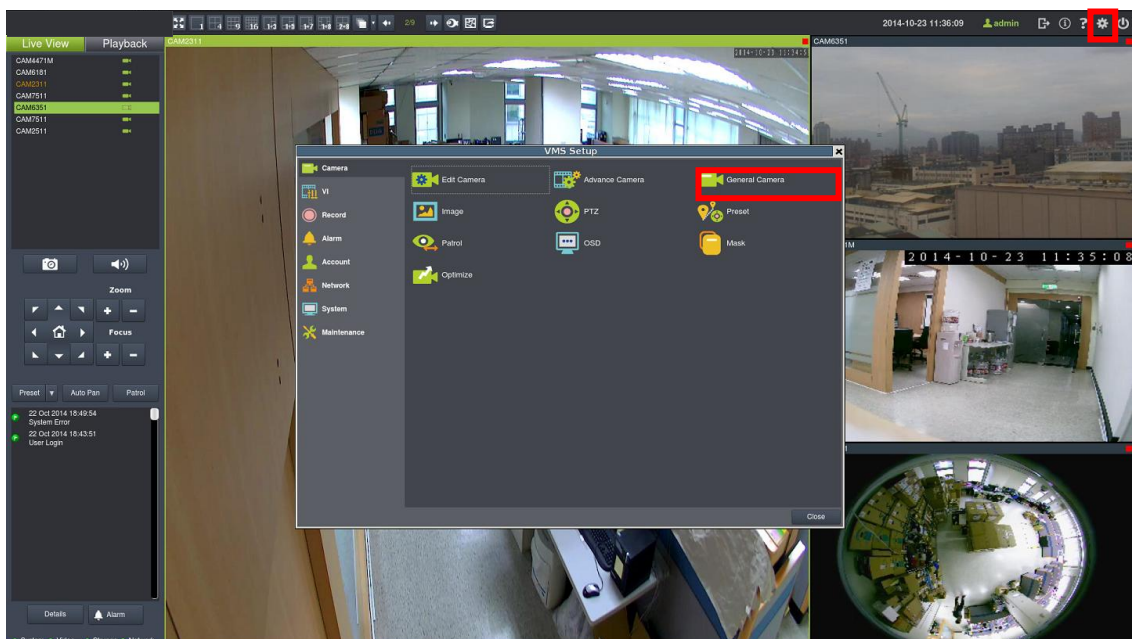
8.2.1. General Camera Settings

Camera general settings include network connectivity settings, as well as basic camera name, description and icon settings.

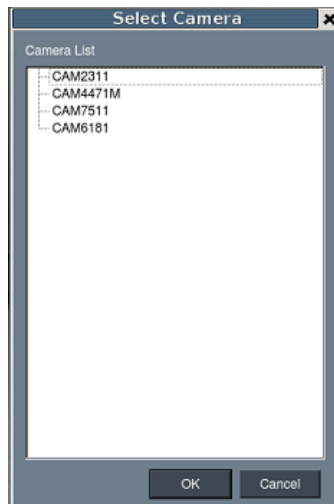
1. Right-click the camera entry and select **Camera Settings > General Camera Settings**.



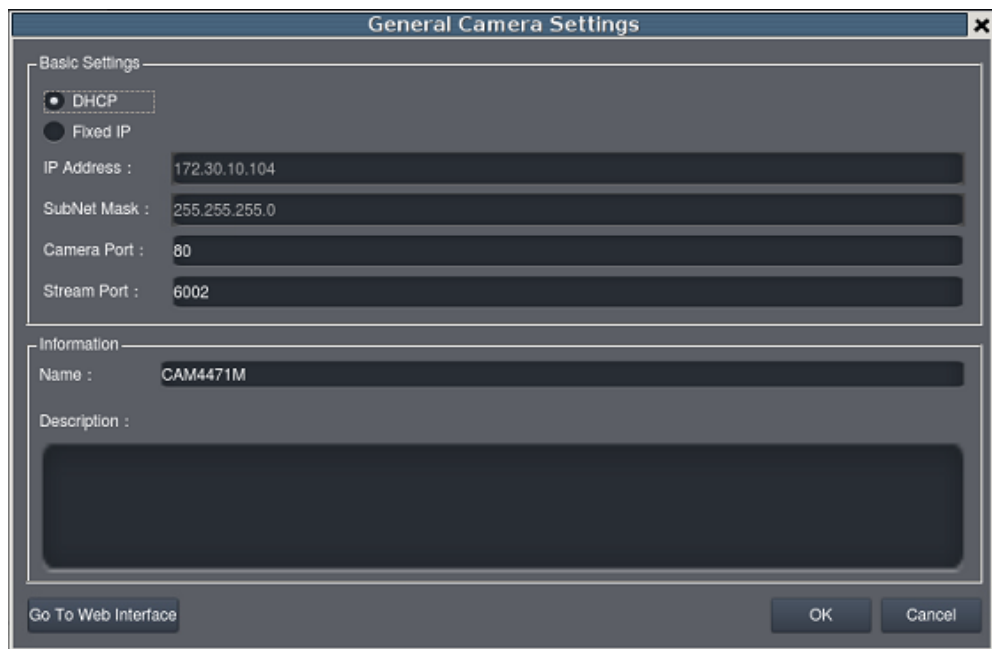
Or click  to bring out **VMS Setup** window and select **Camera** and then select **General Camera**.



Select a specific camera for general setting.



2. There are two ways to specify the IP address for the camera.



- If you wish to automatically assign an IP address to the camera, use DHCP services.
- If you wish to assign a fixed IP, select Fixed IP Address, and provide an IP address for the camera in the IP Address field. The Subnet Mask will be shown together with the IP address.

3. You may continue by editing any of the following options:

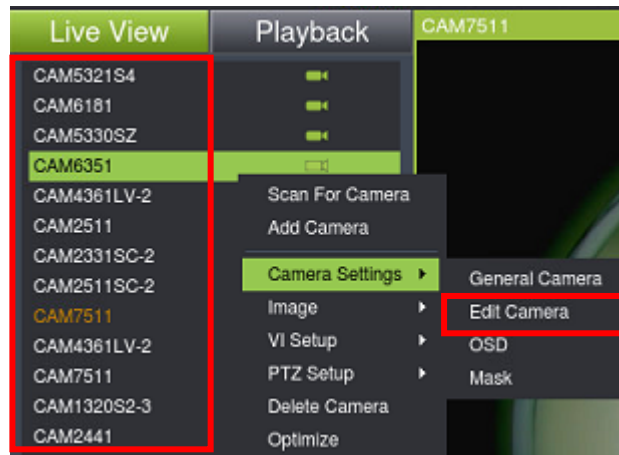
- **Subnet Mask** - a logically visible subdivision of an IP network.


- **Camera Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **Stream Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **Camera Name** - It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**

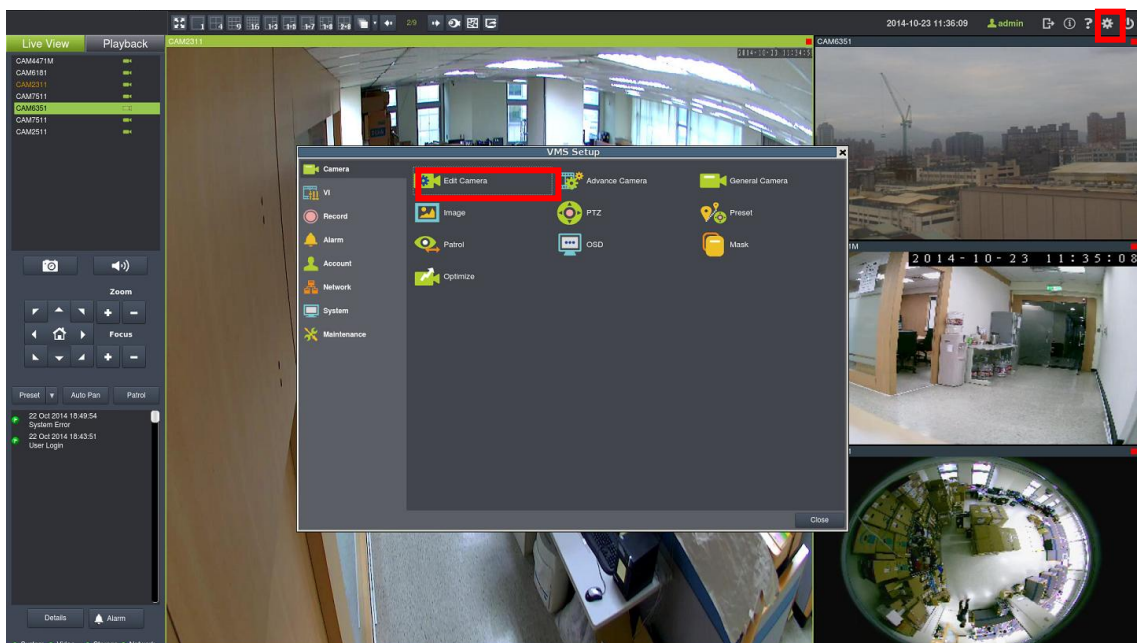
4. Click **OK** to save your changes.

8.2.2. Edit Camera

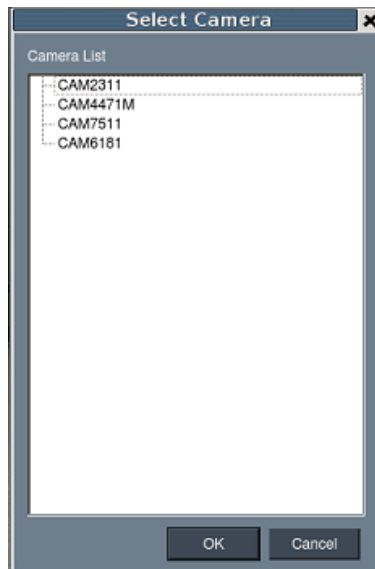
1. Right-click the camera entry and select **Camera Settings > Edit Camera** for settings to the selected camera.



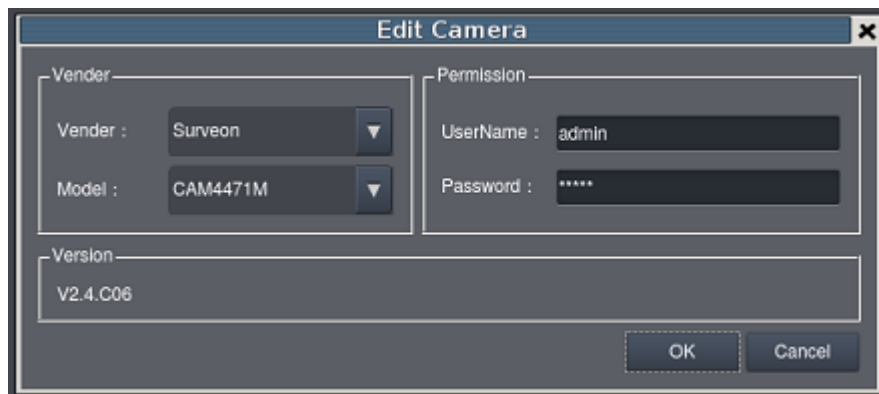
Or click  to bring out **VMS Setup** window and select **Camera** and then select **Edit Camera**.



Select a specific camera for editing.



2. In the *Permissions* section, enter a valid username in the **User Name** field and password in the **Password** field.



Note: The system will not perform an active check on the username and password. Setting an incorrect username or password may affect camera connectivity and configurability.

3. Changing the Camera Model and Vendor

In certain situations it may be necessary to change the Vendor or Model information for the camera. To perform this operation:

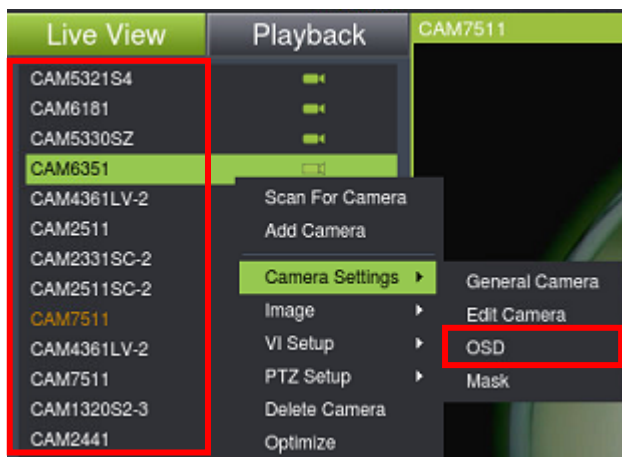
- 3.1. Select the new **Vendor** and **Model** from the respective drop-downs.
- 3.2. Click **OK** to save your changes.


Note: Setting an incorrect vendor or model may affect camera connectivity.

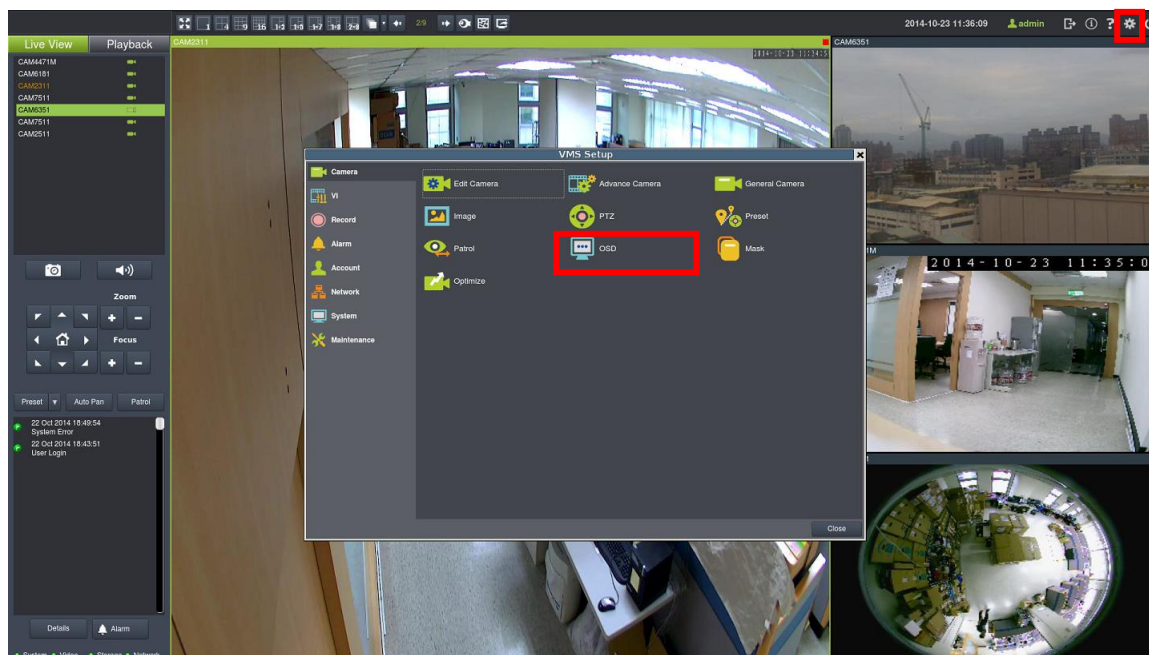
8.2.3. OSD Settings

On cameras with OSD capabilities, these capabilities can be configured within the server. To configure the information for the on-screen display:

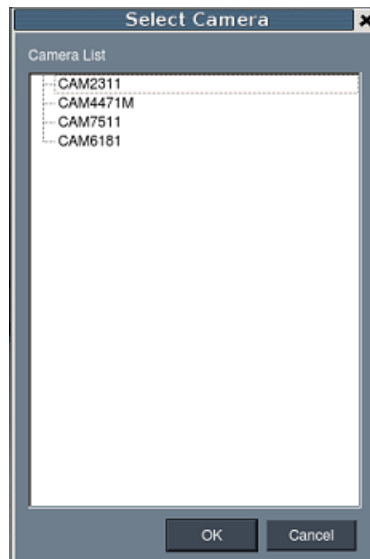
1. Right-click on the specific camera and select **Camera Settings** > **OSD** to bring out the OSD settings menu.



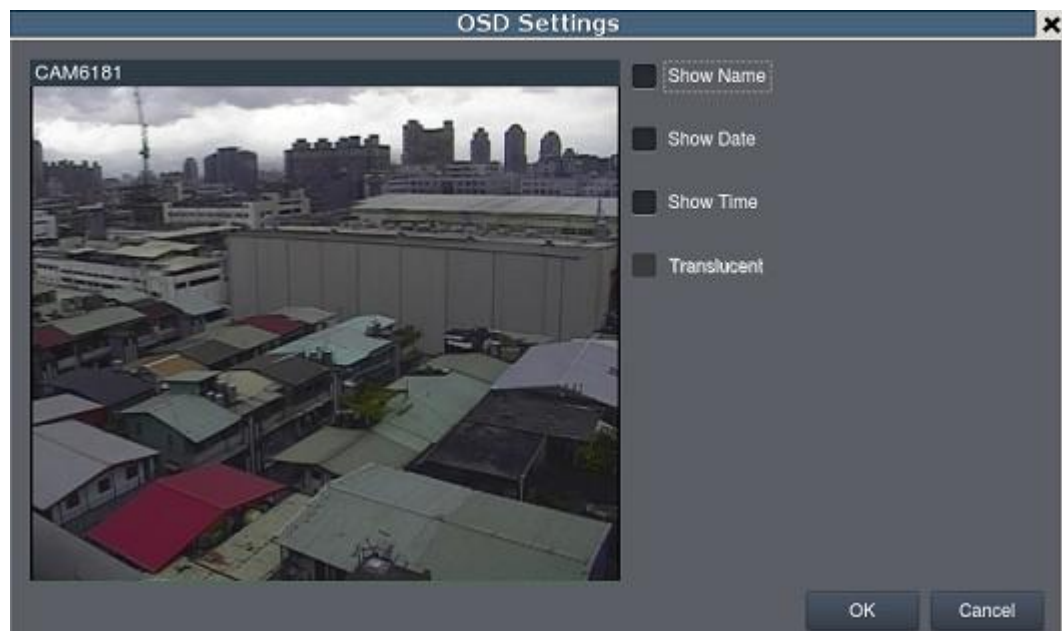
2. Or click  to bring out **VMS Setup** window and select **Camera** and then select **OSD**.



Select a specific camera for OSD settings.



3. Choose any of the following options:

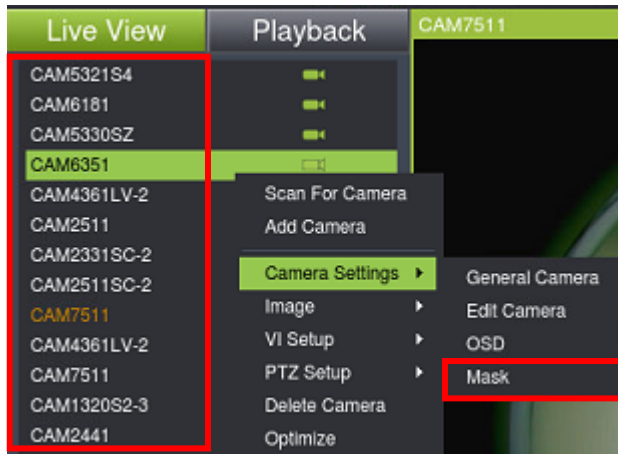



- **Show Name** - Displays the input text on video.
- **Show Date** - Displays the camera date.
- **Show Time** - Displays the camera time.

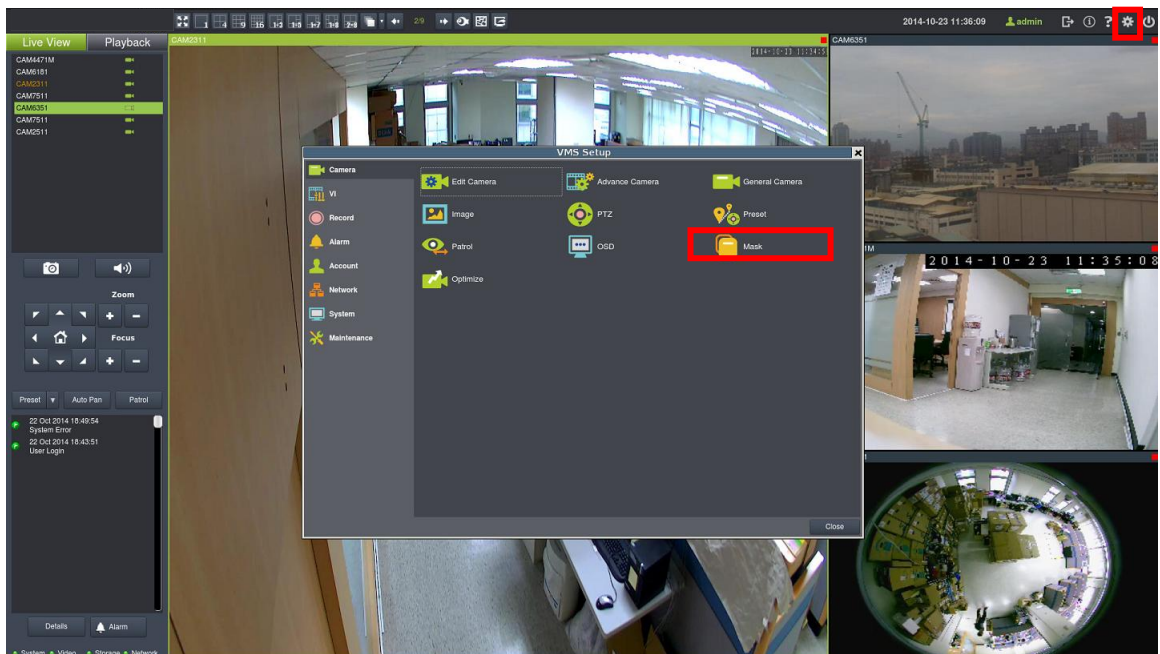
8.2.4. Privacy Mask Settings

Privacy masks can be added on the video:

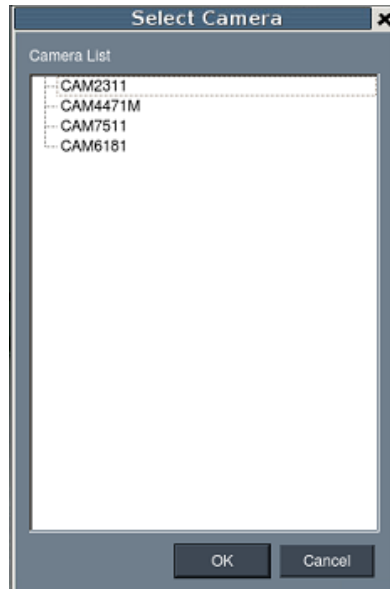
1. Right-click on the specific camera and select **Camera Settings > Mask** to bring out the privacy mask settings menu.



Or click  to bring out **VMS Setup** window and select **Camera** and then select **Mask**.



Select a specific camera for Privacy Mask settings.



1. Click the New Region button to create a new privacy mask overlay, denoted by a border.
2. Click and drag the overlay to move the overlay around the screen. Click and drag one of the six dots on the border to resize and reshape the overlay. If multiple windows are present, the window being edited will have a red border.
3. Repeat these steps to create up to three windows. Click OK to save the privacy mask.

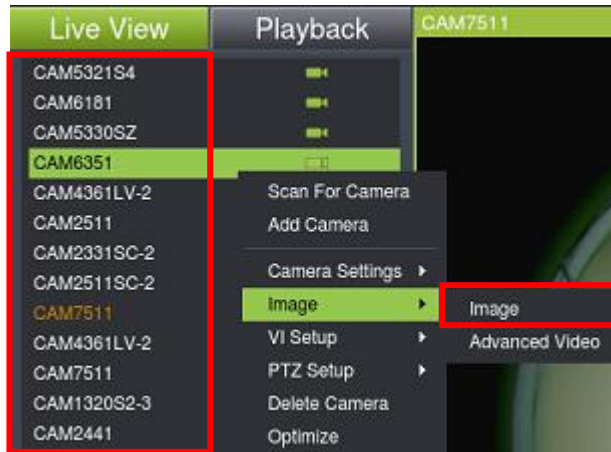
The masked areas will be shown in black on the live view screen after the mask is saved.


8.3. Camera Image and Quality Settings

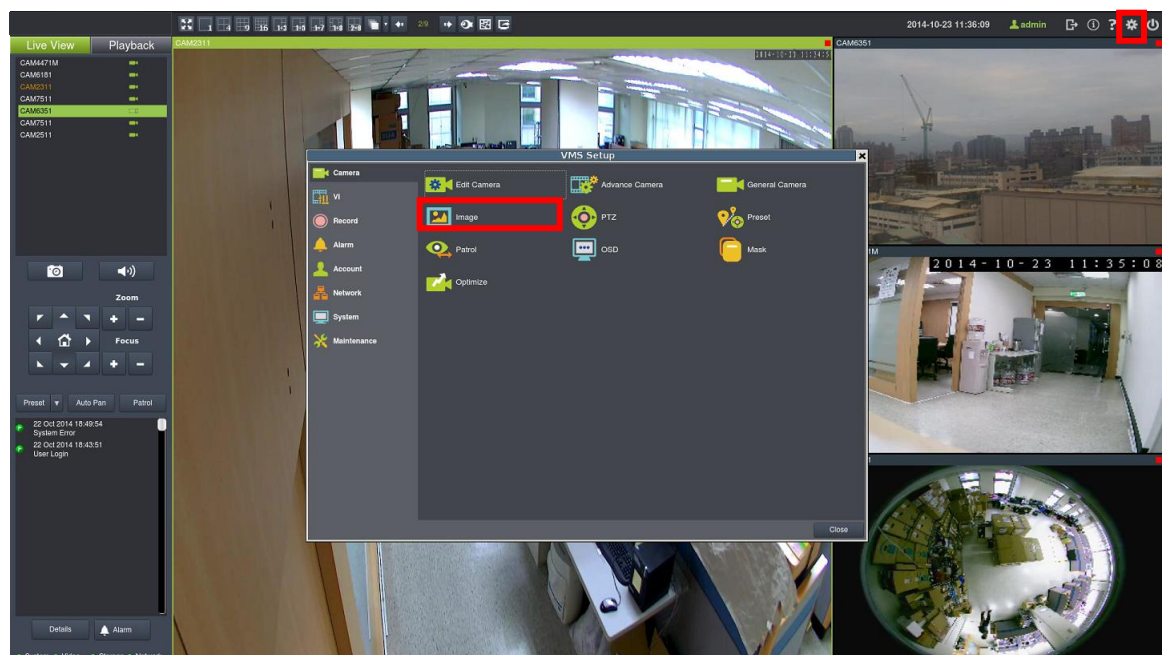
8.3.1. Camera Image Settings

To configure camera image settings:

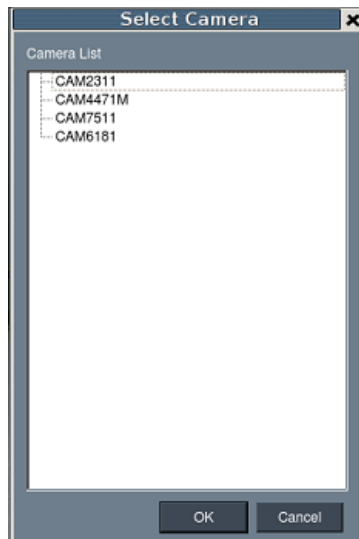
Right-click the specific camera entry and click **Image Adjustments > Image Settings**.



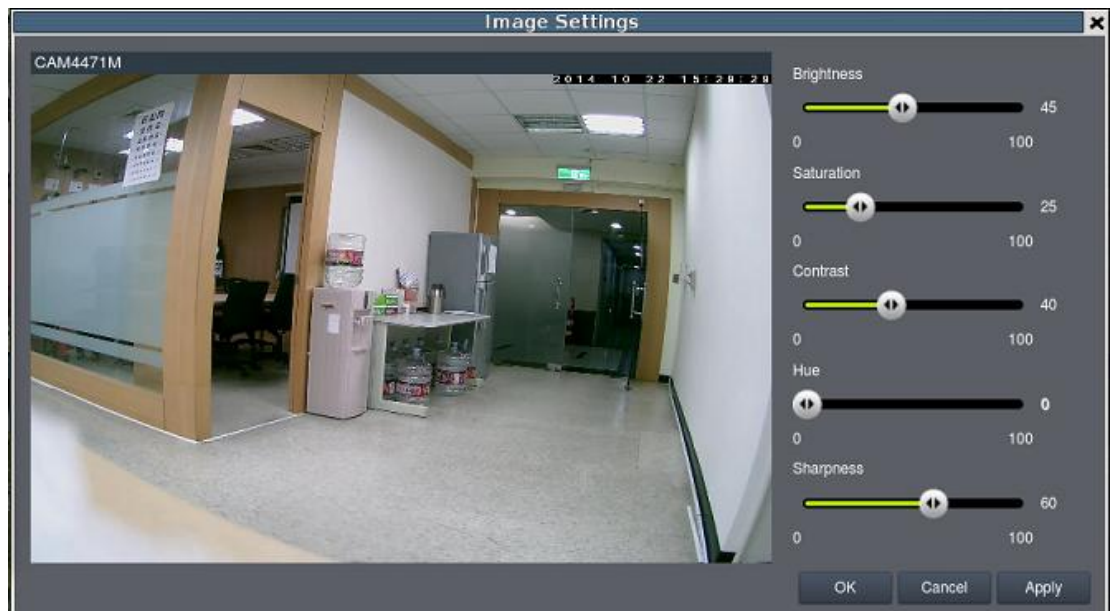
Or click  to bring out **VMS Setup** window and select **Camera** and then select **Image**.



Select a specific camera for image settings.



Note: You must be logged into the camera before changing settings or else the operation will fail.



2. Adjust the following sliders to change the camera image:

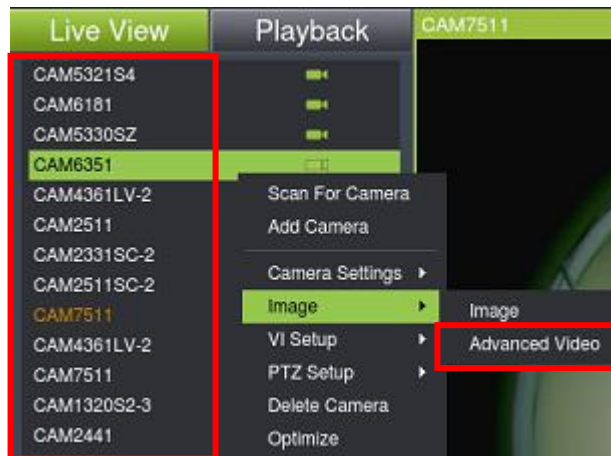
- **Brightness** - The overall lighting level of the image. This value can be used to boost or reduce the apparent lighting of the image.
- **Saturation** - The overall color intensity of the image. This value can be used to boost or reduce overall color intensity.


- **Contrast** - The lighting difference between dark and light areas of the image. This value can be used to boost or reduce apparent differences in lighting.
- **Hue** - The color cast of the image. This value can be used to compensate for colored lighting or other color casting.
- **Sharpness** - The edge contrast of the image. This value can be used to make the picture appear clearer.

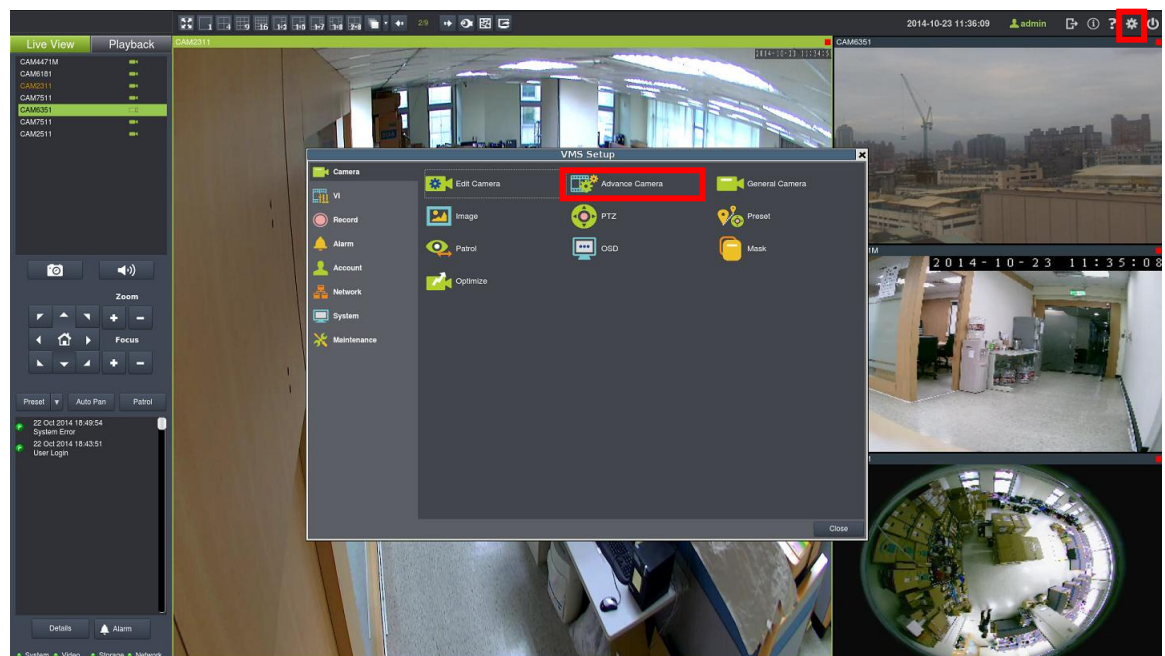
3. Click **OK** to save your changes.

8.3.2. Advanced Video Settings

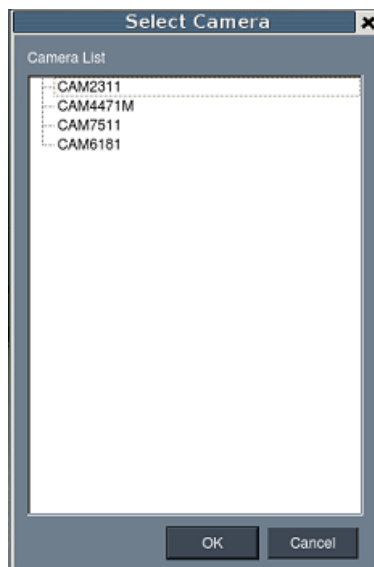
1. Right-click the specific camera entry in the *Camera List* below the *Live View*, then click **Image Adjustments > Advanced Video Settings**.



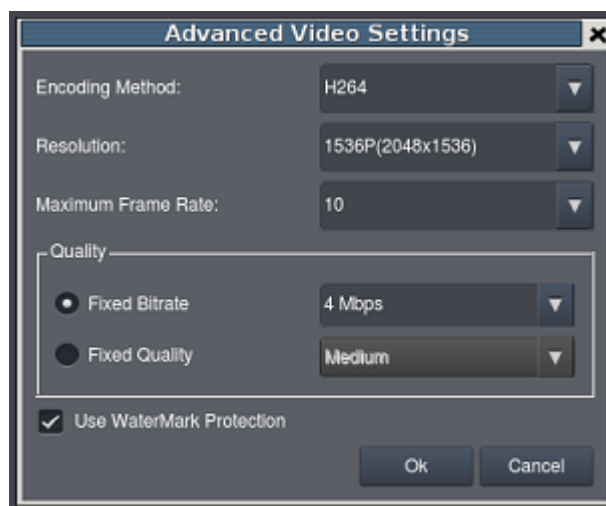
Or click  to bring out **VMS Setup** window and select **Camera** and then select **Advanced Camera**.



Select a specific camera for advanced camera settings.



Note: You must be logged into the camera before changing settings or else the operation will fail.



2. Select a video encoding method from the **Encoding Method** drop-down. Encoding methods will vary by camera type, but common ones include:
 - **MJPEG**
 - **H264**
3. Select a video resolution from the **Resolution** drop-down. Supported resolutions will vary by camera.

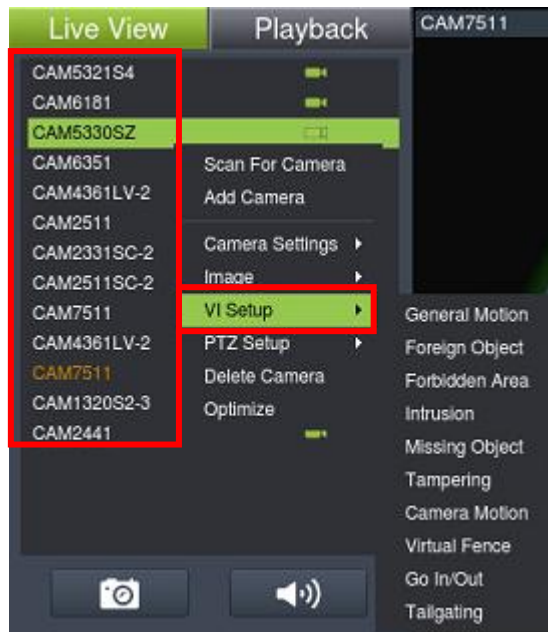
4. Select the Select the maximum video frame rate from the **Maximum Frame Rate** drop-down.

5. From the *Quality* section, choose one of the following:

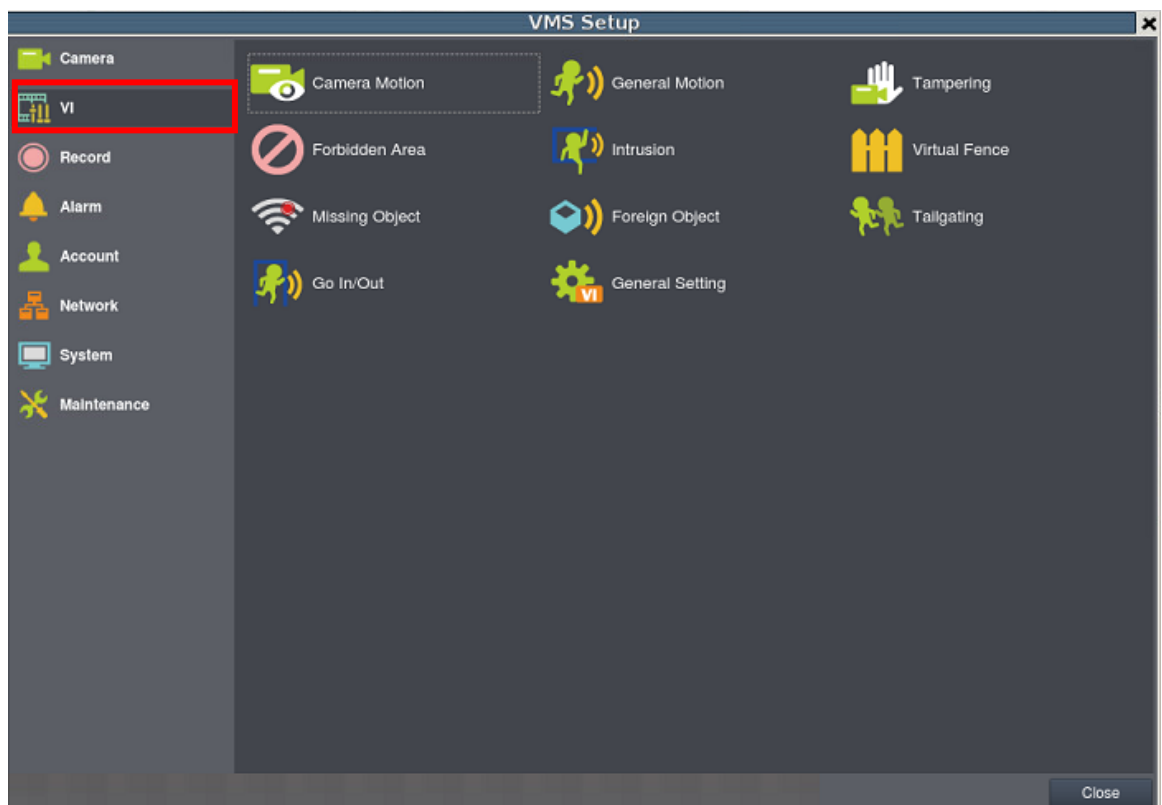
- **Fixed Bitrate** - The camera image quality will be adjusted within a fixed bitrate selected in the dropdown. Dropdown values will vary by camera.
- **Fixed Quality** - The camera bitrate will be adjusted to meet the quality selected in the dropdown. Dropdown values will vary by camera.

8.4. VI Setup

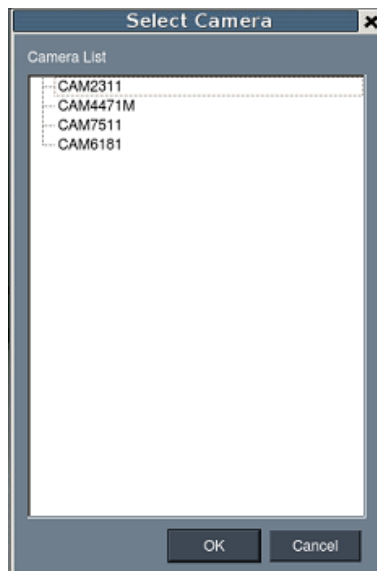
1. Right-click the specific camera entry in the *Camera List* below the *Live View*, then click **Image Adjustments > VI Setup**.



Or click  to bring out **VMS Setup** window and select **VI**.



Select a specific camera for VI Setup.



8.4.1. Camera Motion Detection

Camera motion detection involves using the camera hardware to analyze the video feed and detect motion in specified areas.



Configuring and Editing Detection Windows

To configure a new detection window:

1. Right click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Camera Motion Detection**.

Note: You must be logged into the camera before changing settings or else the operation will fail.

2. If a new window is desired, enter a name in the **New Window Name** field and click the **New** button. Up to 3 detection windows can be set for each camera. The current window will be highlighted.
3. Click and drag the window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. Adjust the sliders: (Settings will be applied to all existing windows)
 - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
 - **Percentage** - Adjusts the amount of the window that must change before an event is triggered.
6. Click **Apply** to save the changes and **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Camera Motion Detection** option.
2. Click the X at the top right corner of the window to delete the window.
3. Click **OK** to save the changes and exit the popup.

8.4.2. General Motion Detection

Automatically detect the moving target entering the security area. When it moves, an alarm will be triggered.



Enabling or Disabling a Detection

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > General Motion Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > General Motion Detection**.
2. If a new window is desired, click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. Adjust the sliders: (Settings will be applied to all existing windows)

- **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
- **Trigger Threshold** - Adjusts the amount of change allowed before and event is triggered.

6. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

1. Right-click the camera entry in the *list of the Live View*, then highlight and click the **VI Setup > General Motion Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any moving objects detected.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

Deleting a Detection Window

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > General Motion Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.3. Tampering Detection

Tampering detection involves using the software to determine when the camera has been improperly moved or redirected.



Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Tampering Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring Tampering Detection

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Tampering Detection**.
2. Adjust the sliders:
 - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
 - **Trigger Threshold** - Adjusts the amount of change allowed before an event is triggered.
3. Click **OK** to save the changes and exit the popup.

Testing Tampering Detection

To test a detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Tampering Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border if tampering is detected.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

8.4.4. Forbidden Area Detection

Forbidden area detection involves using the software to analyze the video feed and immediately detect any object in specified areas.



Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Forbidden Area Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Forbidden Area Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.

5. If an object size has not yet been defined, select **Define the Size of the Detected Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of objects that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)
 - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
 - **Interval** - Adjusts how much time between each check of the forbidden area.
8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Forbidden Area Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any objects detected in the forbidden area.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Forbidden Area Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.5 Intrusion Detection

Intrusion detection involves using the software to analyze the video feed and detect intrusion larger than a certain size.



Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Intrusion Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Intrusion Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.

5. If an object size has not yet been defined, select **Define the Size of the Detected Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of the intrusion that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)
 - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
 - **Duration (Sec)** - Adjusts how much time an object is missing before an event is triggered.
8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Camera List below the Live View, then highlight and click the **VI Setup > Intrusion Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Intrusion Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.6. Virtual Fence

Virtual fence involves using the software to create a fence-crossing detection of the demanding object.



Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Virtual Fence** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Virtual Fence**.

If a new window is desired, select **Directions** and click the **New Region** button to create a new window. The current window will be highlighted with a one/two-way arrow (blue means “in”, green means out”)

2. Click and drag the white arrows along the window border around the one/two-way arrow to resize the space between the fences/adjust the length of the fences.
3. Turn the window border with the orange arrow to change the directions of the fences.
4. If an object size has not yet been defined, select **Define the Size of the Detected Object** and click the **New Region** button to create an object box.
5. Click and drag the corners of the object box to define the minimum size of the fence-crossing objects that will be detected.
6. Adjust the sliders: (Settings will be applied to all existing windows)
 - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
 - **Duration (Sec)** - Adjusts how much time between each check for the fence-crossing.
7. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Camera List below the Live View, then highlight and click the **VI Setup > Virtual Fence** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any difference; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button to enable test detection. During testing a red border will appear if an object goes missing.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

4. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Virtual Fence** option.
5. Highlight an existing detection window.
6. Click the **Clear** button to delete the window.
7. Click **OK** to save the changes and exit the popup.

8.4.7. Missing Object Detection

Missing object detection involves using the software to analyze the video feed and detect missing objects larger than a certain size.



Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Missing Object Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Missing Object Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.

4. Click the interior of a window to drag it to the desired position.
5. If an object size has not yet been defined, select **Define the Size of the Detected Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of the missing objects that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)
 - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
 - **Duration (Sec)** - Adjusts how much time an object is missing before an event is triggered.
8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Camera List below the Live View, then highlight and click the **VI Setup > Missing Object Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a border will appear if a object goes missing.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Missing Object Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.8. Foreign Object Detection

Foreign object detection involves using the software to analyze a video feed and detect objects that do not belong.



Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Foreign Object Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click OK to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Foreign Object Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.

4. Click the interior of a window to drag it to the desired position.
5. If an object size has not yet been defined, select **Define the Size of the Detected Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of objects that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)
 - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
 - **Duration** - Adjusts the amount of time before an object triggers an event.

Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Foreign Object Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any foreign objects detected.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

Deleting a Detection Window

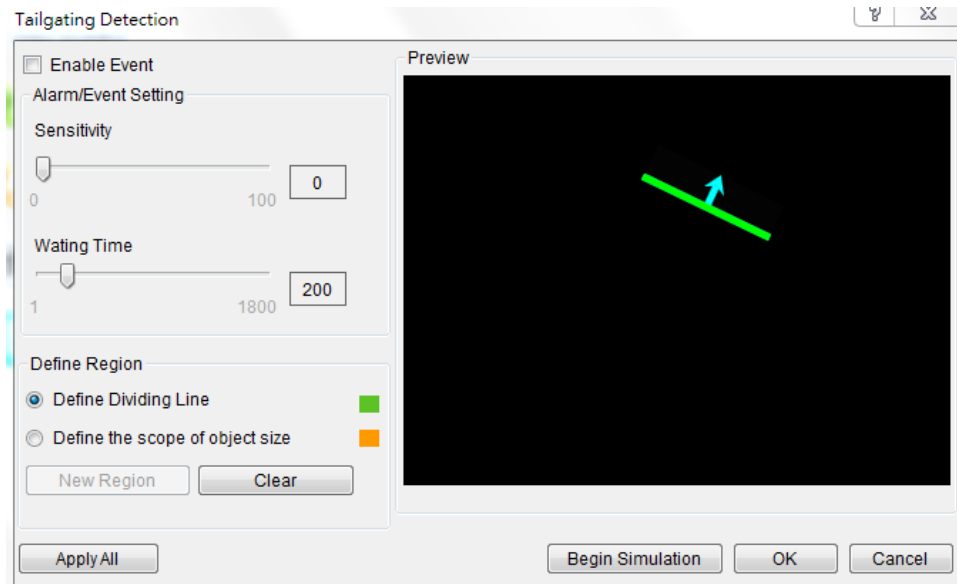
To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Foreign Object Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.

8.4.9. Tailgating Detection

This functionality is currently available for remote client only.

Tailgating detection involves using the software to analyze the video feed and detect a tailgating object crossing over the restricted area.



Note: Tailgating Detection can also be configured by clicking *Camera List > Video Analytics > Tailgating Detection* in the VMS Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click *VI Setup > Tailgating Detection*.
2. If a new window is desired, select *Define Dividing Line* and click the *New Region* button to create a new dividing line. Only 1 dividing line can be set for each camera.
3. Click and drag the created dividing line to the desired position and direction.
4. If an object size has not yet been defined, select *Define the Size of the Detected Object* and click the *New Region* button to create an object box.
5. Click and drag the corners of the object box to define the minimum size of the objects that will be detected.
6. Adjust the sliders: (Settings will be applied to all existing windows)

6. Sensitivity - Adjusts window sensitivity from 0 (low) to 100 (high).
7. Waiting Time (Sec) - Adjusts how much time an object is tailgating before an event is triggered.
7. Click OK to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Setup > Tailgating Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Dividing Line

To delete a new dividing line:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Setup > Tailgating Detection** option.
2. Highlight the dividing line.
3. Click the **Clear** button to delete the line.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

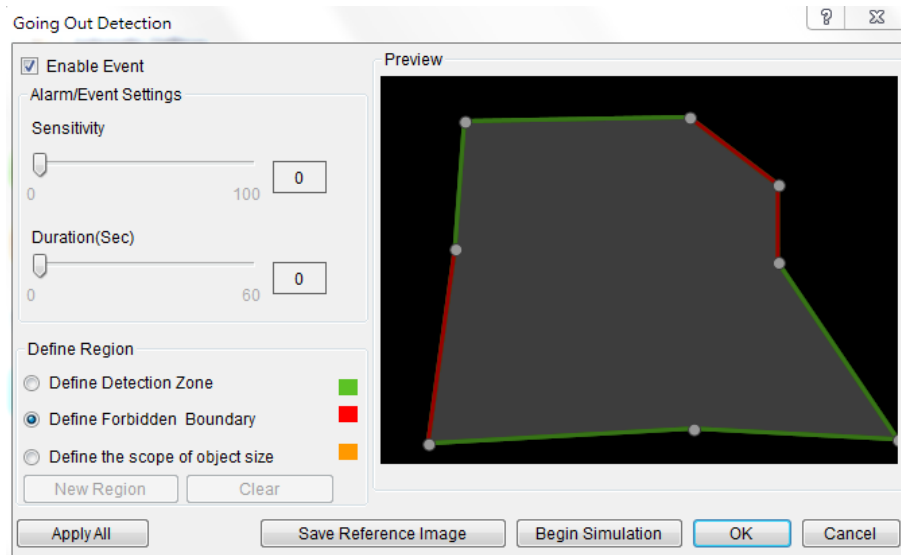
To enable or disable the detection functions:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Setup > Tailgating Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

8.4.10. Go In/Out Detection

This functionality is currently available for remote client only.

Go in/out detection involves using the software to analyze the video feed and detect a go in/out object crossing over the restricted area.



Note: Go In/Out Detection can also be configured by clicking *Camera List > Video Analytics > Go In/Out Detection* in the VMS Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click *VI Setup > Go In/Out Detection*.
2. If a new window is desired, select *Define Detection Zone* and click the *New Region* button to create a new window. Only 1 detection window can be set for each camera.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to mark the restricted line; once clicked, the clicked line will turn red. The red lines are the boundaries. Up to 8 boundaries can be set.
5. If an object size has not yet been defined, select *Define the Size of the Detected Object* and click the *New Region* button to create an object box.

6. Click and drag the corners of the object box to define the minimum size of the objects that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)
8. Sensitivity - Adjusts window sensitivity from 0 (low) to 100 (high).
9. Duration (Sec) - Adjusts how much time an object is missing before an event is triggered.
8. Click OK to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Setup > Go In/Out Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Setup > Go In/Out Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

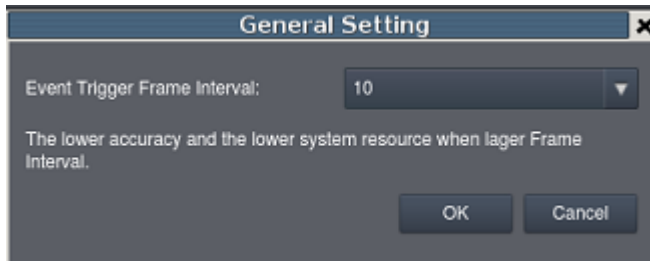
To enable or disable the detection functions:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Setup > Go In/Out Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.

8.4.111. General Settings

Set the event trigger frame interval here.

It takes less system resources for bigger trigger frame intervals but the accuracy will be lower.



8.5. PTZ Setup

In cameras equipped with any combination of pan, tilt or zoom (PTZ) functionality, these settings are used to configure the PTZ functions.

8.5.1. PTZ Setup

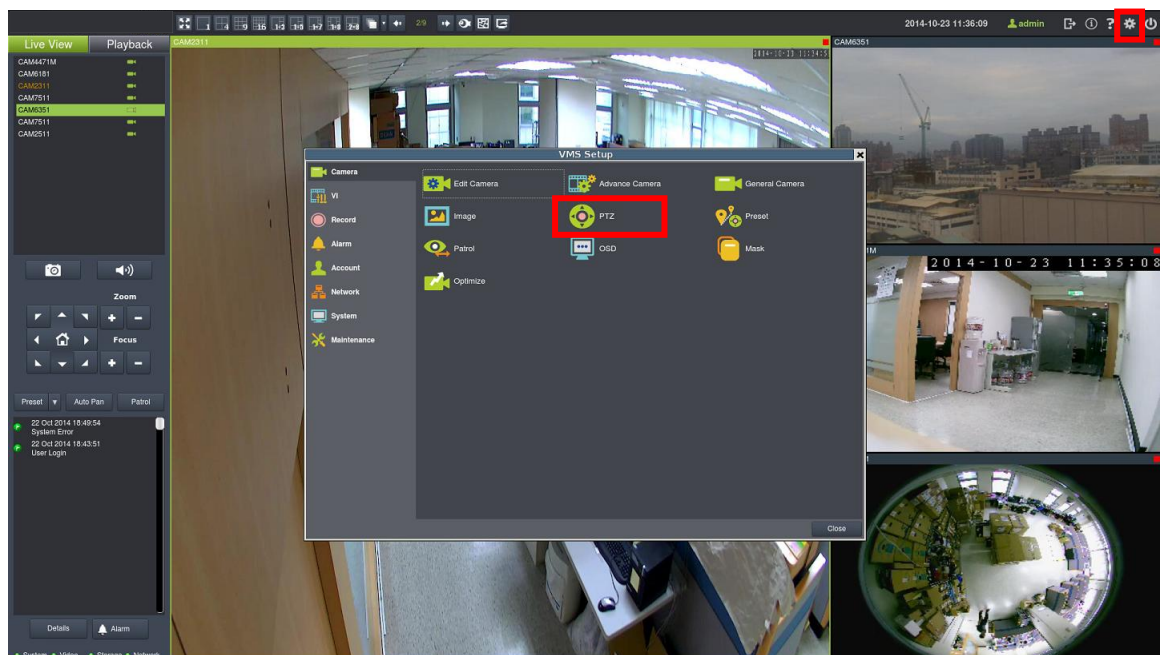
The PTZ Setup deal with the software PTZ control panel. These settings adjust how much the camera will pan, tilt, zoom, and focus with each control panel input.

Note: You must be logged into the camera before changing settings or else the operation will fail.

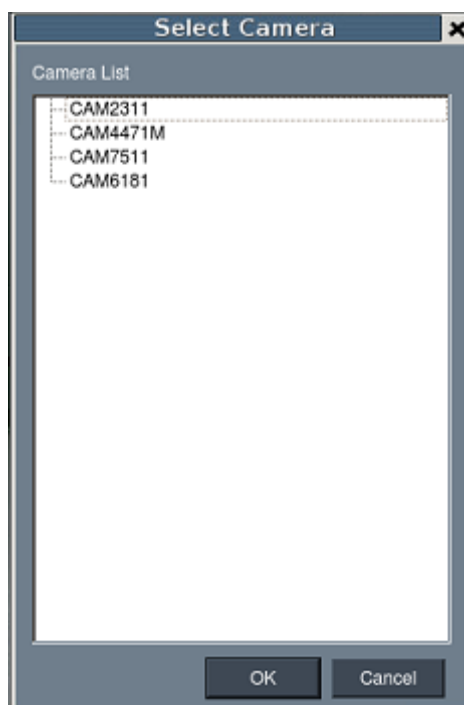
1. Right-click the specific camera with the PTZ functionality and click **PTZ Setup > PTZ**.



Or click  to bring out **VMS Setup** window and select **Camera** and then select **PTZ**.

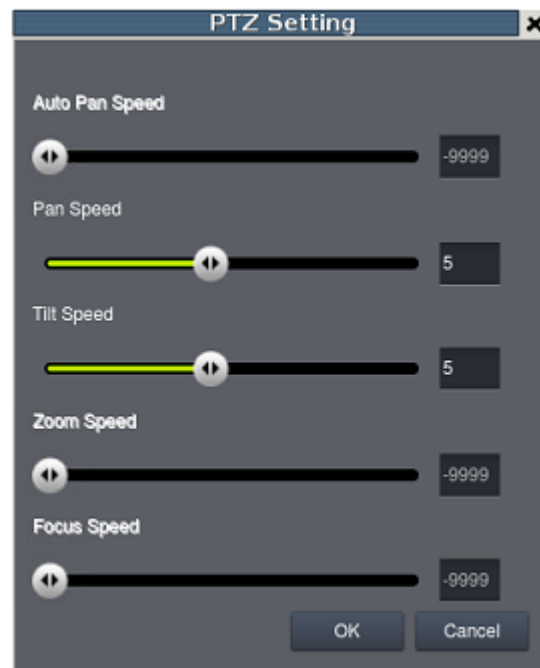


Select a specific camera for advanced camera settings.



Note: You must be logged into the camera before changing settings or else the operation will fail.

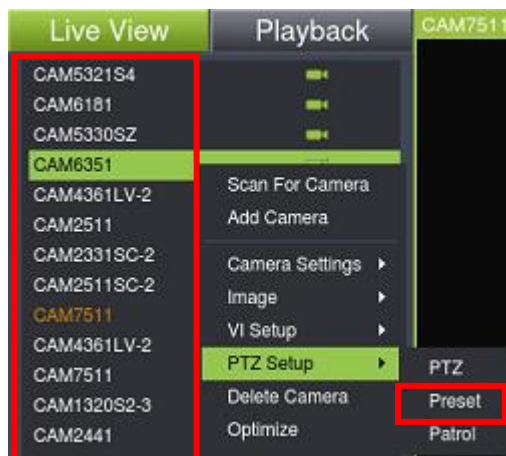
2. Adjust the following sliders to increase and decrease the following speeds: (The higher the value, the higher the speed) Unsupported features on specific cameras will be grayed out.




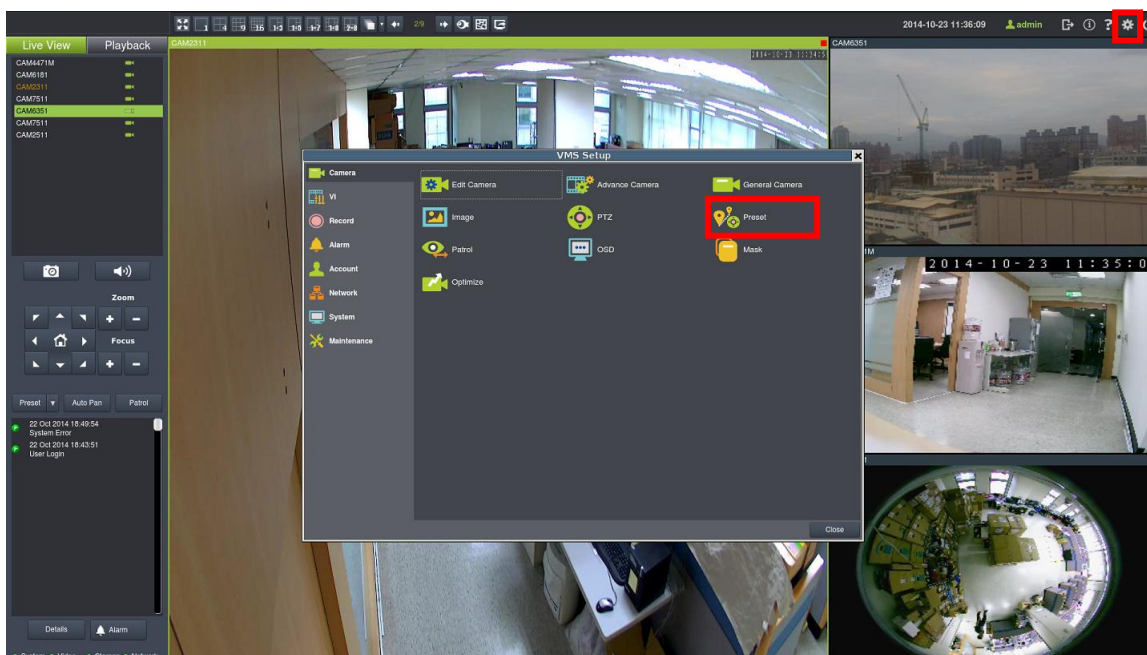
- **Auto Pan Speed** - The speed which the camera will pan between the mechanical stops when the **Auto Pan** function is activated.
- **Pan Speed** - The distance the camera will pan to each side.
- **Tilt Speed** - The distance the camera will tilt up and down.
- **Zoom Speed** - The distance the camera will zoom near or far.
- **Focus Speed** - The amount the camera will focus forward or backward.

8.5.2. PTZ Preset Settings

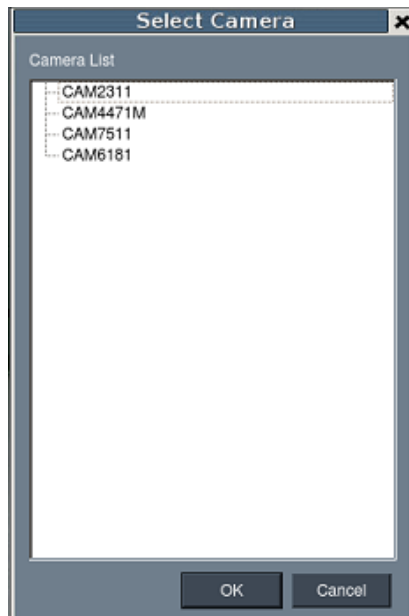
Certain preset pan/tilt/zoom values can be saved in order to move the camera quickly to a point of interest. To configure camera PTZ preset settings, right-click the specific camera with the PTZ functionality, then highlight and click **PTZ Setup** > **Preset** option.



Or click  to bring out **VMS Setup** window and select **Camera** and then select **Preset**.

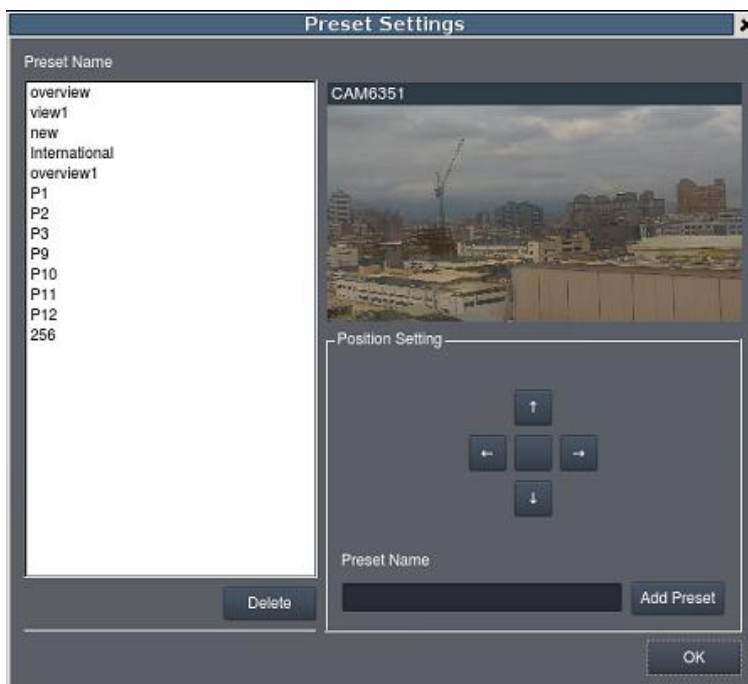


Select a specific camera for advanced camera settings.



Note: You must be logged into the camera before changing settings or else the operation will fail.

The popup will display the camera output, as well as a *Position Setting* pad.



Note: You must be logged into the camera before changing settings or else the operation will fail.

Adding a Preset

1. Use the directional pad to move the camera view. Use the center “home” button to return the camera to the default zeroed view.
2. Once the camera reaches the point where a preset is desired, type a name into the **Preset Point Name** field.
3. Click the **Add a preset point** to add the preset to the list. Click **OK** exit the menu, or you may continue to add/delete additional presets.

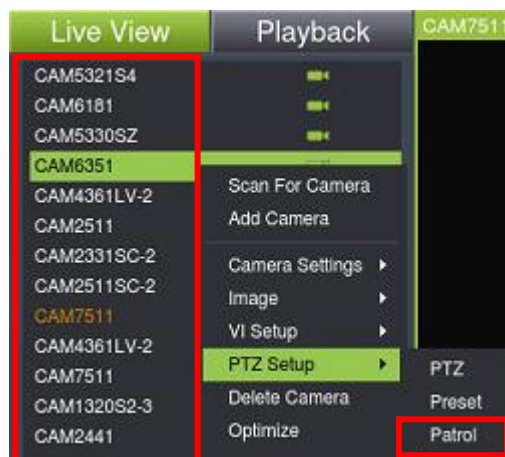
Deleting a Preset

To delete a preset, simply highlight the preset and click the **Delete** button. Click the **Yes** button to confirm deletion. Click **OK** exit the menu, or you may continue to add/delete additional presets.


8.5.3. PTZ Patrol Settings

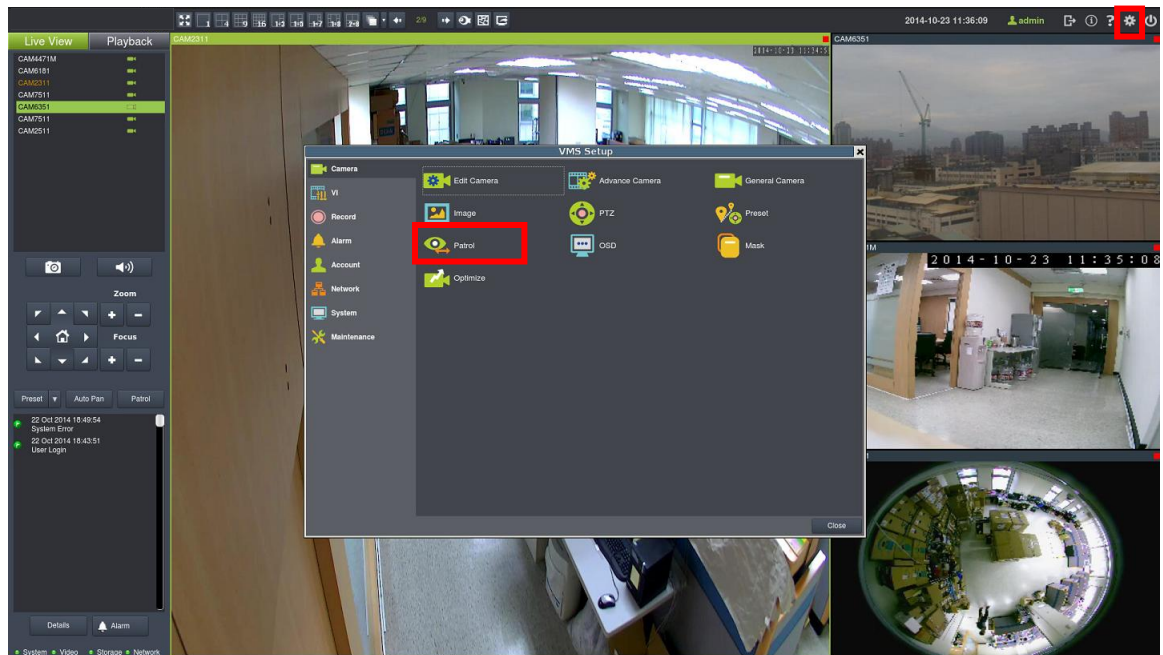
In cameras with PTZ functionality, one camera can be used to survey a large area. This can be done automatically using the patrol functionality. This function basically moves the camera between preset points in a fixed pattern. To configure camera patrol settings:

1. Right-click the specific camera with the PTZ functionality, highlight and click the **PTZ Setup > Patrol Settings**.

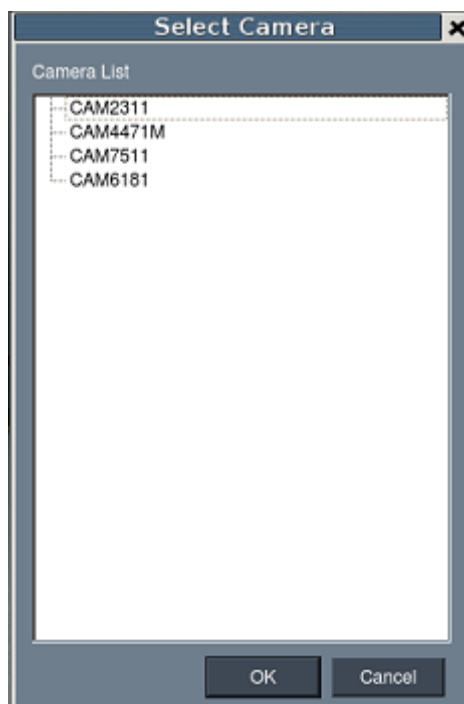


Note: You must be logged into the camera before changing settings or else the operation will fail.

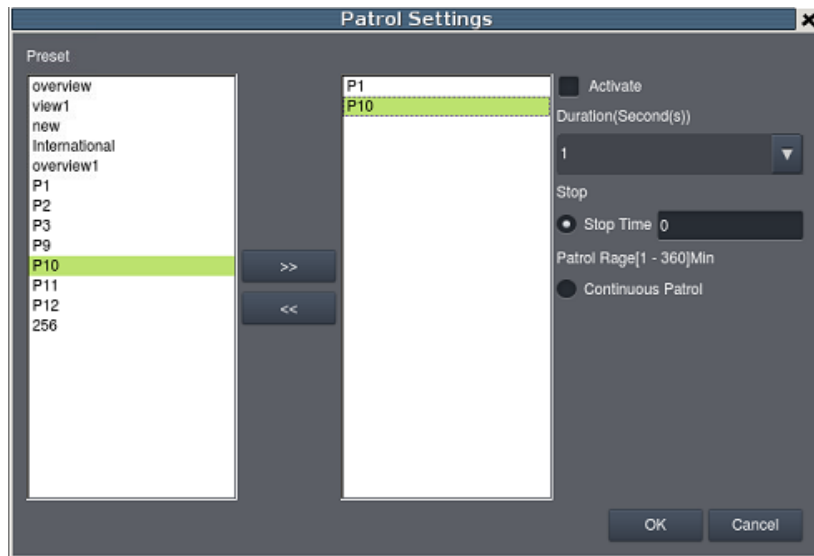
Or click  to bring out **VMS Setup** window and select **Camera** and then select **Patrol**.



Select a specific camera for advanced camera settings.



Note: You must be logged into the camera before changing settings or else the operation will fail.



1. On the right side of the popup there will be a list of preset points that are defined for the camera. Use the >> button to add the points to the patrol list in the order that they are to be viewed. Points can also be removed by highlighting them and clicking on the << button.
2. Select the length of time the camera will dwell at each preset point before continuing from the **Dwelling Time (Sec)** dropdown.
3. Select one of the following:
 - **Stop Time** - The camera will stop the number of minutes specified in the box between patrol sessions.
 - **Continuous Patrol** - The camera will not stop between patrol sessions.
4. Check the **Active** box to activate the patrol list.
5. Click the **OK** button to save the patrol list and exit the popup.

8.5. PTZ Controls

Cameras equipped with Pan-Tilt-Zoom functionality can be controlled directly within the local client software. These controls can be found in the *Live View Control* window within the live view screen.



Note: (1) The camera to be controlled must be selected by highlighting it (clicking its output window) in the main view window.

8.5.1. Directional Pad

Pan and Tilt

The pan and tilt functionalities can be controlled with the directional pad.

Clicking the right or left arrow will pan the camera by one step in the direction clicked. Clicking the up or down arrow will tilt the camera by one step in the direction clicked. Clicking diagonal arrows will combine the pan and tilt action of the adjacent arrows. Clicking on the Home icon, located at the center of the pad, will re-center the camera.

8.5.2. Functional Buttons

Home

One position can be set as the Home position. Click on Home button to go to the Home position. Clicking on the Home button will re-center the camera.

Preset

The camera may have preconfigured viewpoints, or presets configured. To switch to one of these presets, click the **Preset** button and select the preset.

Auto Pan

The camera will start or stop pan between the mechanical stops.

Patrol

In cameras with PTZ functionality, one camera can be used to survey a large area. This can be done automatically using the patrol functionality.

Zoom

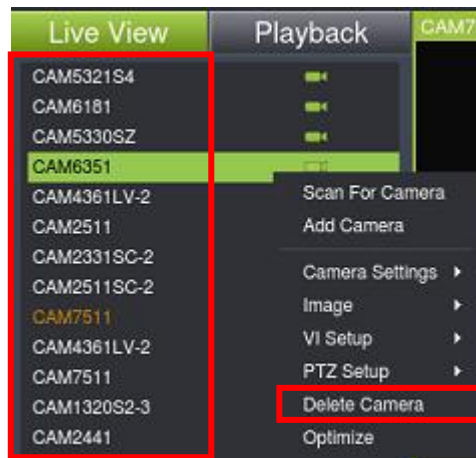
The zoom on a camera can be controlled with the + and - buttons located inside the direction pad. Pressing the + button will increase zoom distance by 1 step. Pressing the - button will decrease zoom distance by one step.

Focus

The focus on a camera can be controlled with the + and - buttons located beside the *Focus* box. Pressing the + button will increase focus distance by 1 step. Pressing the - button will decrease focus distance by one step.

8.5.3. Deleting a Camera

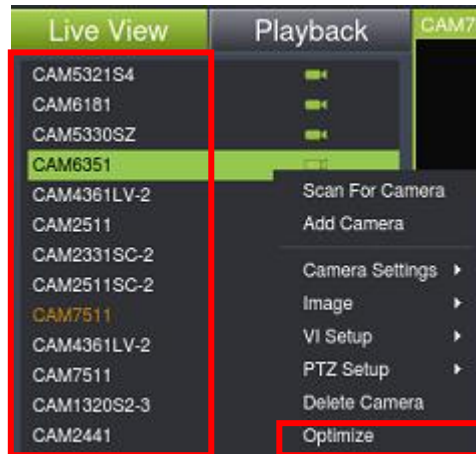
1. Right-click the camera entry you wish to remove to bring out the options popup. Highlight and click the **Delete Camera** option.




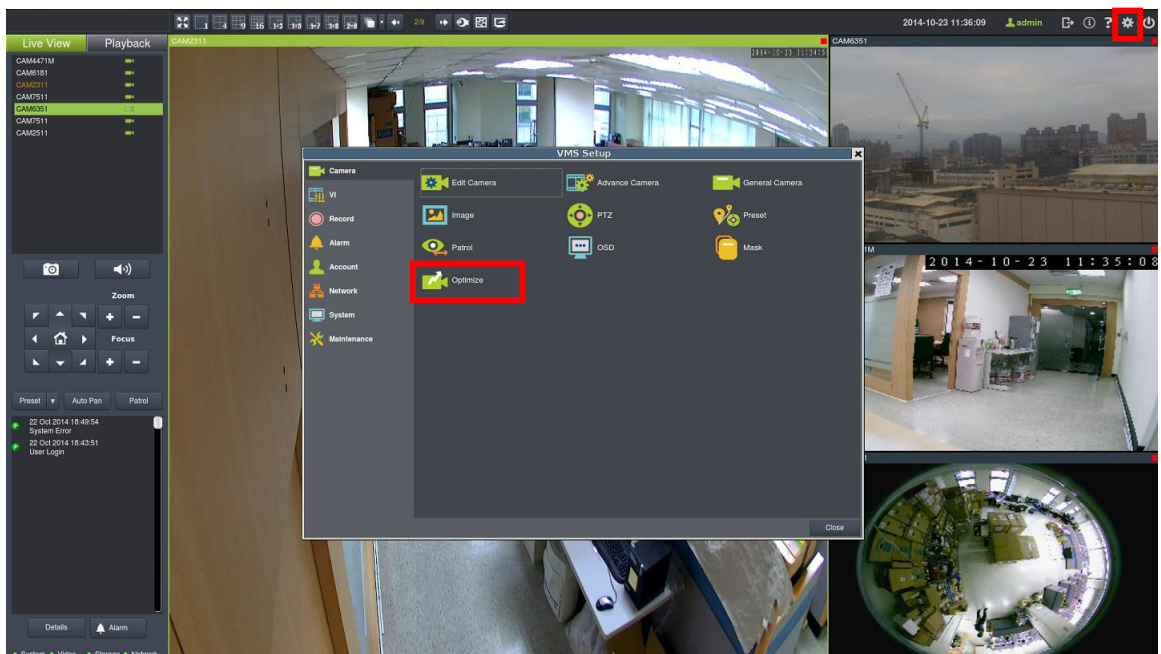
8.5.4. Optimizing a Camera

Optimizing the camera resets the camera so that it will correspond to the settings on the Server. To perform this operation:

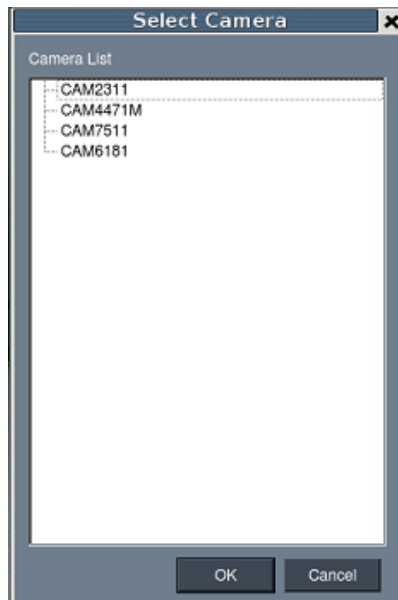
1. Right-click the camera entry you wish to remove to bring out the options popup. Highlight and click the **Optimize** option.



Or click  to bring out **VMS Setup** window and select **Camera** and then select **Optimize**.



Select a specific camera for advanced camera settings.




Note: You must be logged into the camera before changing settings or else the operation will fail.

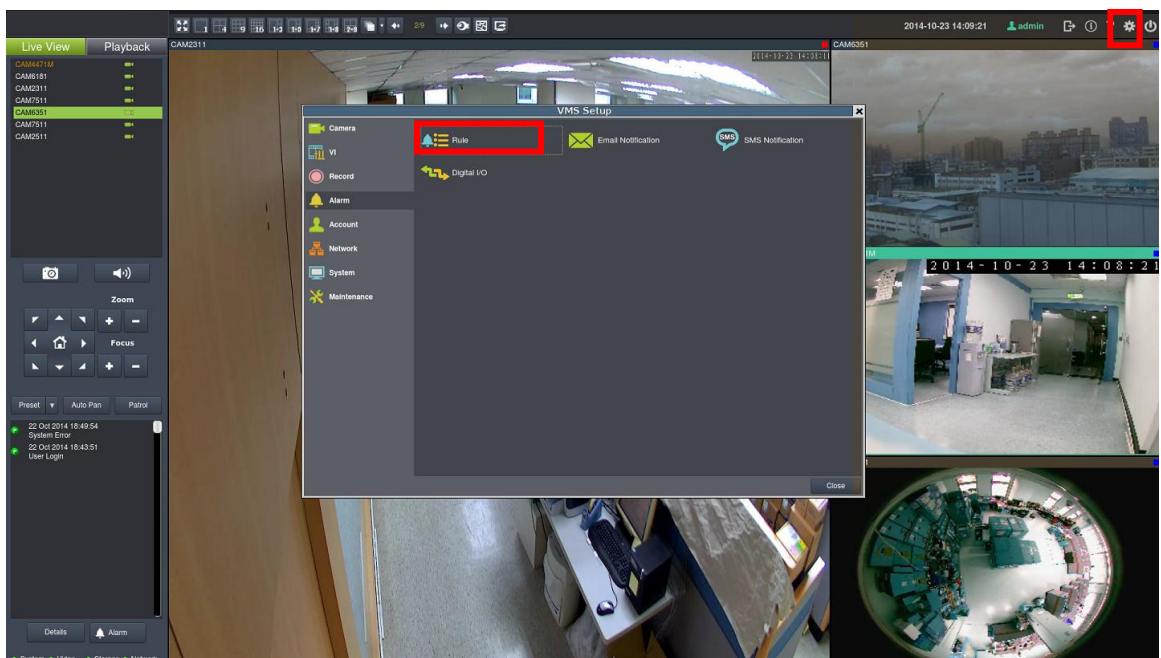
Chapter 9. Alarms and Events

This section will guide the user through the detection setup and digital Inputs for detecting alarm conditions, the setup of digital outputs and alarm popups and notifications, as well as the setup of alarm rules and schedules.

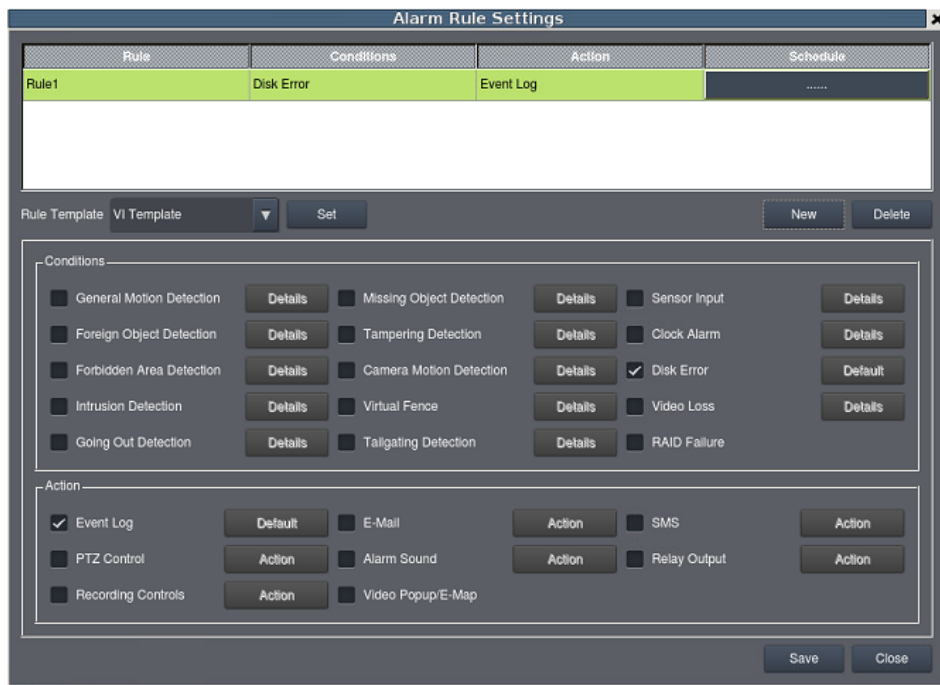
9.1. Alarm Rules

VMS Client provides robust alarm handling features.

To access these features click  to bring out **VMS Setup** window and select **Alarm** and then **Rules**.



In the Alarm Rules, you can combine the alarm trigger conditions with action items such as event notification, video recording, and/or camera movements. Multiple alarm rules can be created using the following elements:

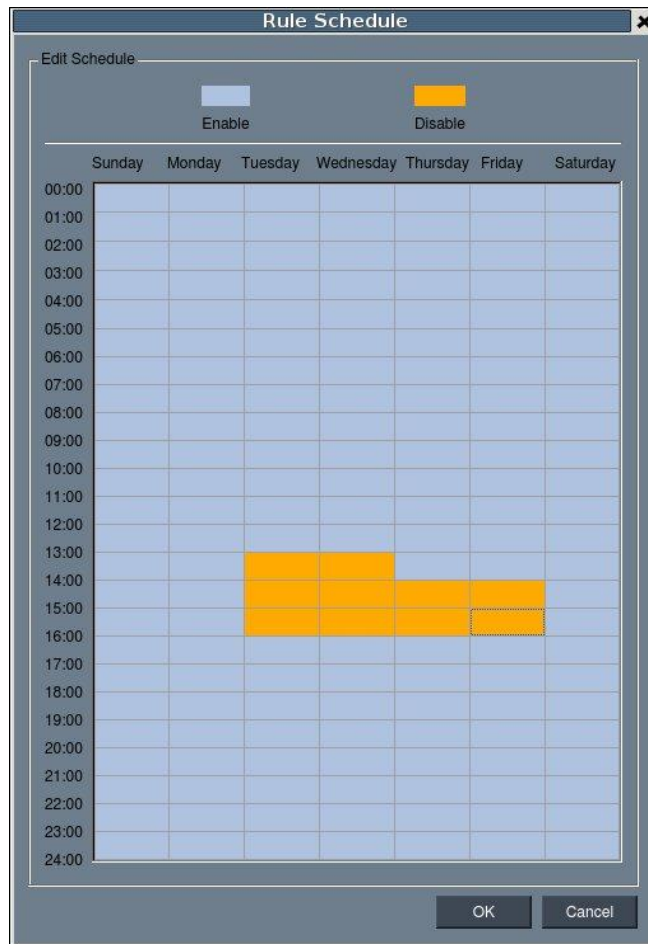


Alarm handling in the VMS is divided into 4 distinct phases:

1. **Rule:** An alarm rule combines conditions with corresponding actions.
2. **Condition:** The condition is the triggering event for the alarm such as Motion/Video loss/Sensor Input/Clock Alarm, etc.
3. **Action:** Specifies steps and actions that can be undertaken when an alarm is triggered.
4. **Schedule:** Allows the user to schedule the application of specific alarm rules. This is useful in cases such as applying rules to non-office hours.

9.1.1. Adding an Alarm Rule

1. Click the **New** button.
2. Enter a short description for the new rule in the **Add Rule** field.
3. Choose conditions and actions. Click the button in the alarm field to set up a schedule for the rule. These selections are described in the following sections.



4. Click the **Save** button to save the rule.

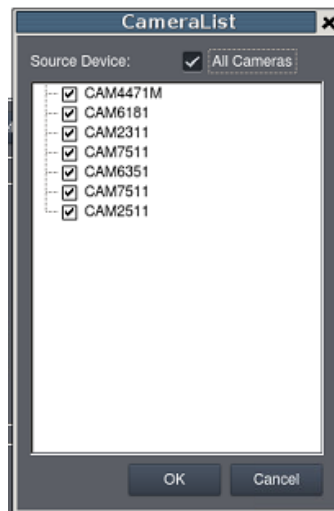
Conditions

The follow alarm conditions can be set to trigger the alarm:

When configuring a camera, a detection area can be specified for the following detections: General Motion Detection / Foreign Object Detection / Forbidden Area Detection / Intrusion Detection / Go In/Out Detection / Missing Object Detection / Tampering Detection / Camera Motion Detection / Virtual Fence / Tailgating Detection.

After the detection area is specified, detection can be activated and an alarm handling scheme configured in this menu.

Clicking on the **Detail** button will pull up a menu listing all the devices with General Motion Detection active.



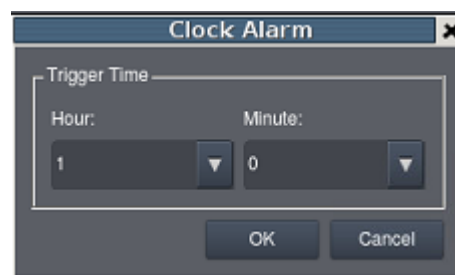
From this menu, click the checkboxes next to the cameras that have General Motion Detection configured. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

Sensor Input

The alarm is triggered by a sensor input. For example this may include doorway entry sensors that are connected to the camera system. Clicking on the Detail button will pull up the *Sensor Input Settings* menu, listing all the cameras. From this menu, click the checkboxes next to the cameras that will be used to trigger the Alarm. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

Clock Alarm

When a preset time is reached, the alarm is triggered. The Clock Alarm is triggered only on the day it is configured. Clicking on the **Detail** button will pull up the *Clock Alarm* menu.



From this popup select the hour and minute the alarm will be triggered. Click the **OK** button to exit the menu.

Disk Error

The alarm is triggered when a disk drive failure occurs.

Video Loss

When video input is lost, the alarm is triggered. Clicking on the **Details** button will pull up the *Video Loss Settings* menu, listing all the cameras. From this menu, click the checkboxes next to the cameras that will be used to trigger the Alarm. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

Actions

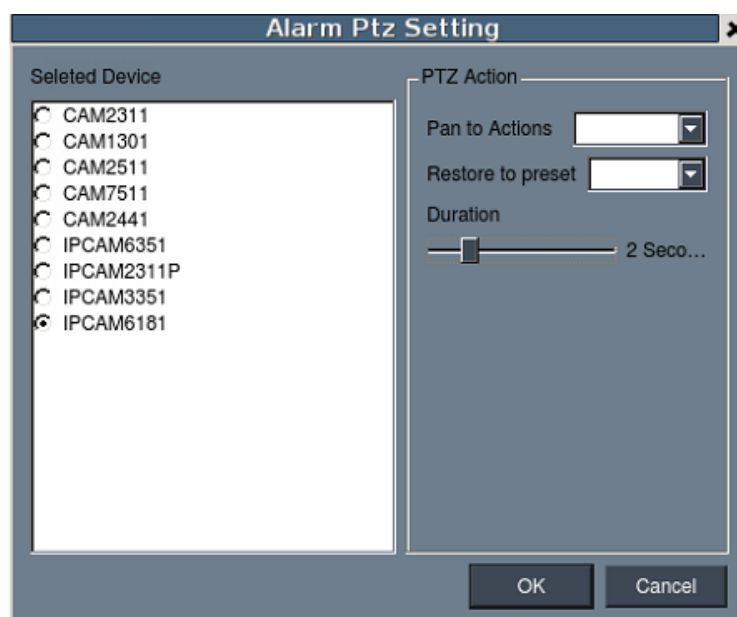
The following alarm actions can be taken when the alarm is triggered:

Event Log

The system issues event messages when the alarm is triggered.

PTZ Control

When the alarm is triggered, a Pan-Tilt-Zoom action can be set to slew the camera to a particular position. For example, clicking on the **Action** button brings up the *PTZ Action Settings* menu. In this menu:



1. Choose a camera from the list.
2. Select a preset point from the **Pan to Preset** dropdown that the camera will pan to.
3. Select the preset that the camera will return to from the **Restore Presets** dropdown.
4. Specify a duration that the camera will stay at the **Pan to Action** preset before returning to the **Restore to Preset** using the **Duration** slider. Click **Apply** to save the settings.
5. Click **OK** to exit the menu.

Recording Controls

When the alarm is triggered, the system records video onto the storage. Clicking on the **Action** button will pull up the *Recording Settings* menu.

Use the checkboxes within to select cameras that will be recorded. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

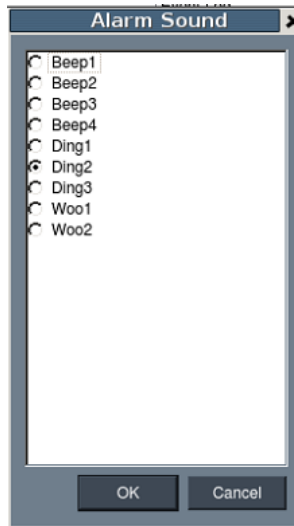
E-Mail

When the alarm is triggered, an E-Mail will be sent. Checking this option will bring up the *E-mail Settings* menu.

1. In the *SMTP Server* tab, under the *E-mail Server* heading, you may either enter the URL (such as smtp.abc.com) or IP address of the SMTP server that the Server will use to deliver E-mail notifications. The SMTP server configured here must support Unicode Transformation Format-8 (UTF-8) encoding.
2. Enter the user name for the Server email account in the **Username** field.
3. Enter the password for the Server email account in the **Password** field.
4. Enter a valid E-mail address in the **Reply Address** field. This address will be the default sender listed in E-mails sent from the Server.
5. Enter one or more E-mail addresses in the **Recipients:** field. These address(es) will receive notifications from the Server. Multiple addresses can be entered by separating individual addresses with semi -colons “;”.
6. Enter the subject of your notification E-mails, e.g., Server-xxxxsite1notification in the **E- Mail Title** field.
7. Enter a short message in the large field to describe the Server or a surveillance network.
8. **(Optional)** Click **Test** to send a test message to the E-mail addresses listed.
9. Click the **OK** button to exit E-mail settings.

Alarm Sound

When the alarm is triggered, the system will play an audible alarm sound. Clicking on the **Action** button will pull up the *Warning Sound* menu, listing available sounds.



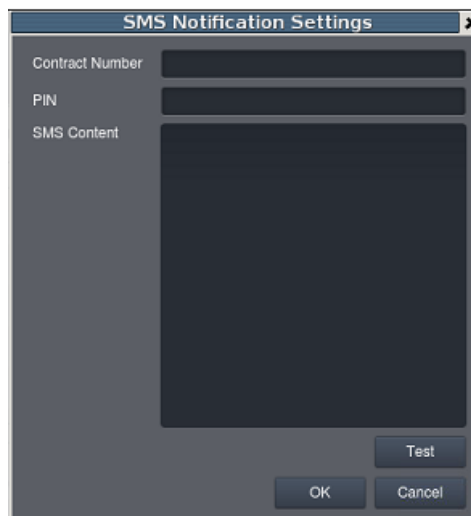
Video Popup / E-Map

When the alarm is triggered, a popup video appears on the local client.

Clicking the **Action** button will pull up a menu.

SMS

When the alarm is triggered, an SMS message will be sent. Checking this option will bring up the *SMS Settings* menu.



Note: Drivers for supported GSM/GPRS modems have already been installed on the server. Currently, only the **WaveCOM-M1206B** is supported. Use COM1 on the Server to connect to a GSM modem.

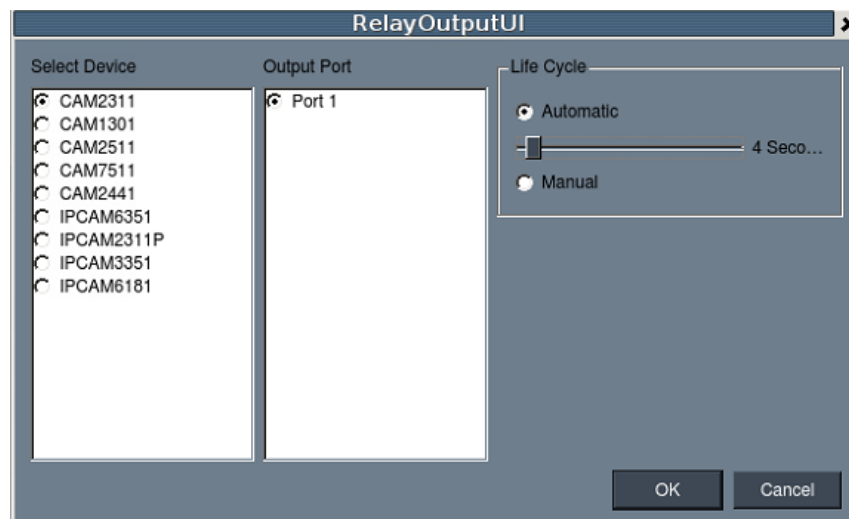
1. In the **Contact Number** field, enter the phone numbers that will receive SMS notifications. Be sure to include the area code, e.g., “86”, in front of phone numbers. Use commas, “,” to separate individual phone numbers.
2. Use the slider bar to select a delay between the occurrence of an event and SMS message delivery.
3. (Optional) If a SIM PIN is required, enter the PIN code in the **PIN** field. Note that applying incorrect PIN code may disable your SIM card.

Note: To change the PIN code, remove the SIM card from your GSM modem. Use a cell phone to change the PIN code and then re -install SIM card into the GSM modem. Changing PIN codes is not recommended because a configuration failure may disable your SIM card.

4. In the **SMS Content** field, type a simple description to include in the outgoing SMS messages
5. (Optional) Click **Test** to send a test message to the phone numbers listed.
6. Click the **Apply** button to apply the changes.
7. Click the **OK** button to exit SMS settings.

Relay Output

When the alarm is triggered, a signal will be relayed to an external source such as a light switch, siren, or other external link. Clicking on the **Action** button brings up the *External Relay Settings* menu. In this menu:



1. Choose a camera from the list.
2. Select an output port to relay to.
3. Select output duration, from 0 to 60 seconds.
4. Click the **OK** button to exit the menu.

Alarm Scheduling

When the alarm is created, click thebutton located in the scheduling column of the alarm listing to bring up the *Alarm Rule Schedule* menu. This displays a table with the days of the week as the columns, and hours as the rows, allowing the user to schedule the alarm on exact hours.

Rule	Conditions	Action	Schedule
Rule1	Disk Error	Event Log

Rule Template: VI Template [v] Set [New] [Delete]

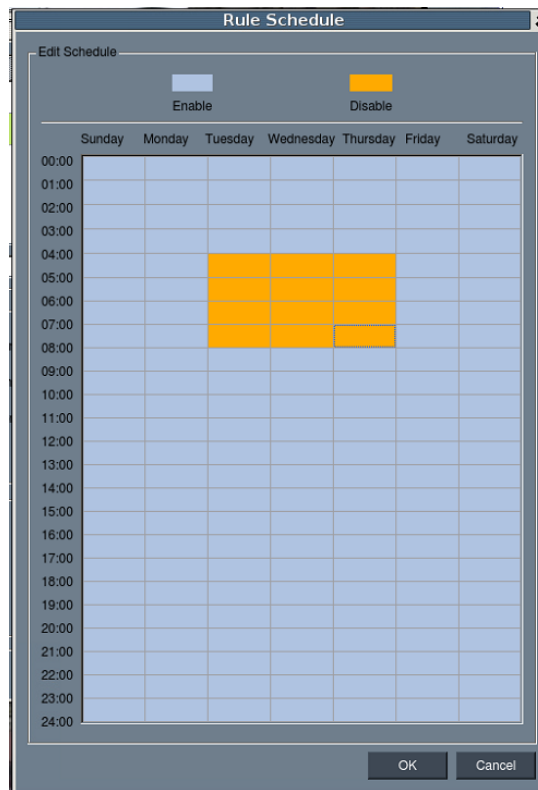
Conditions

<input type="checkbox"/> General Motion Detection [Details]	<input type="checkbox"/> Missing Object Detection [Details]	<input type="checkbox"/> Sensor Input [Details]
<input type="checkbox"/> Foreign Object Detection [Details]	<input type="checkbox"/> Tampering Detection [Details]	<input type="checkbox"/> Clock Alarm [Details]
<input type="checkbox"/> Forbidden Area Detection [Details]	<input type="checkbox"/> Camera Motion Detection [Details]	<input checked="" type="checkbox"/> Disk Error [Default]
<input type="checkbox"/> Intrusion Detection [Details]	<input type="checkbox"/> Virtual Fence [Details]	<input type="checkbox"/> Video Loss [Details]
<input type="checkbox"/> Going Out Detection [Details]	<input type="checkbox"/> Tailgating Detection [Details]	<input type="checkbox"/> RAID Failure

Action

<input checked="" type="checkbox"/> Event Log [Default]	<input type="checkbox"/> E-Mail [Action]	<input type="checkbox"/> SMS [Action]
<input type="checkbox"/> PTZ Control [Action]	<input type="checkbox"/> Alarm Sound [Action]	<input type="checkbox"/> Relay Output [Action]
<input type="checkbox"/> Recording Controls [Action]	<input type="checkbox"/> Video Popup/E-Map	

[Save] [Close]



From this menu, use the following steps to schedule the alarm:

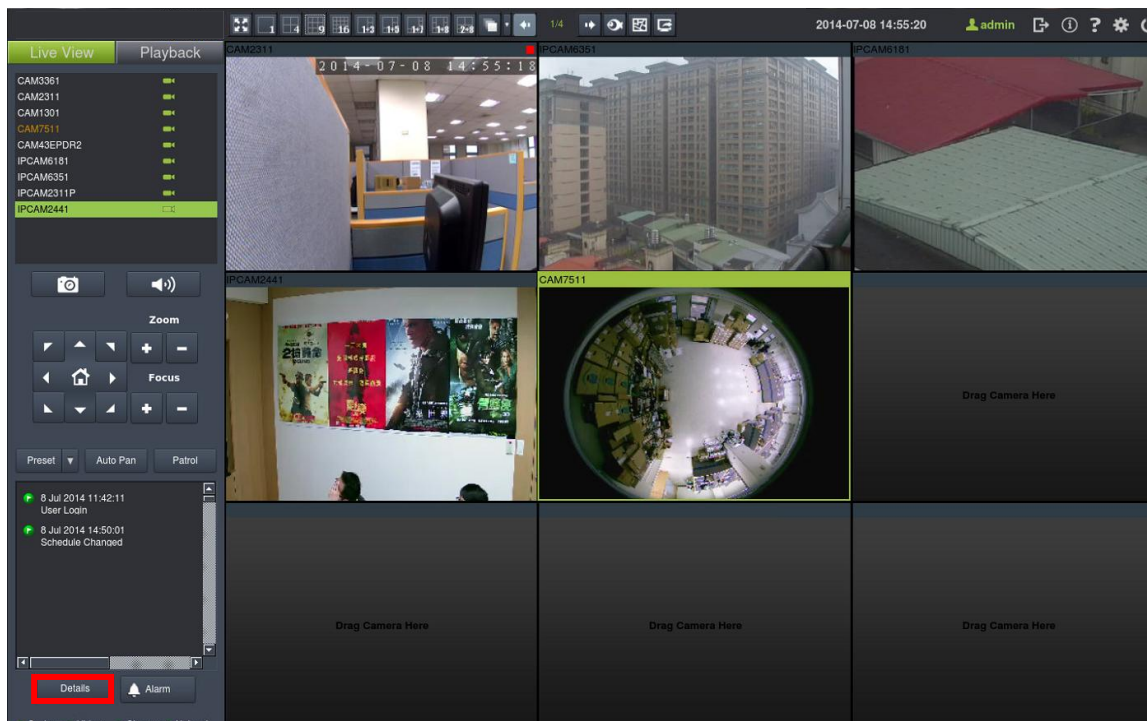
1. Choose the rule that you wish to apply the schedule to.
2. Click the **Enable** or **Disable** button to bring up a “paintbrush.”
3. Click the cursor on the table to “paint” in a schedule. You may click and drag to paint a wide area.


For example, if you wish to disable the alarm on Tuesday at 6pm, you would click the box Tuesday-18:00. Disabled time periods are highlighted in yellow.

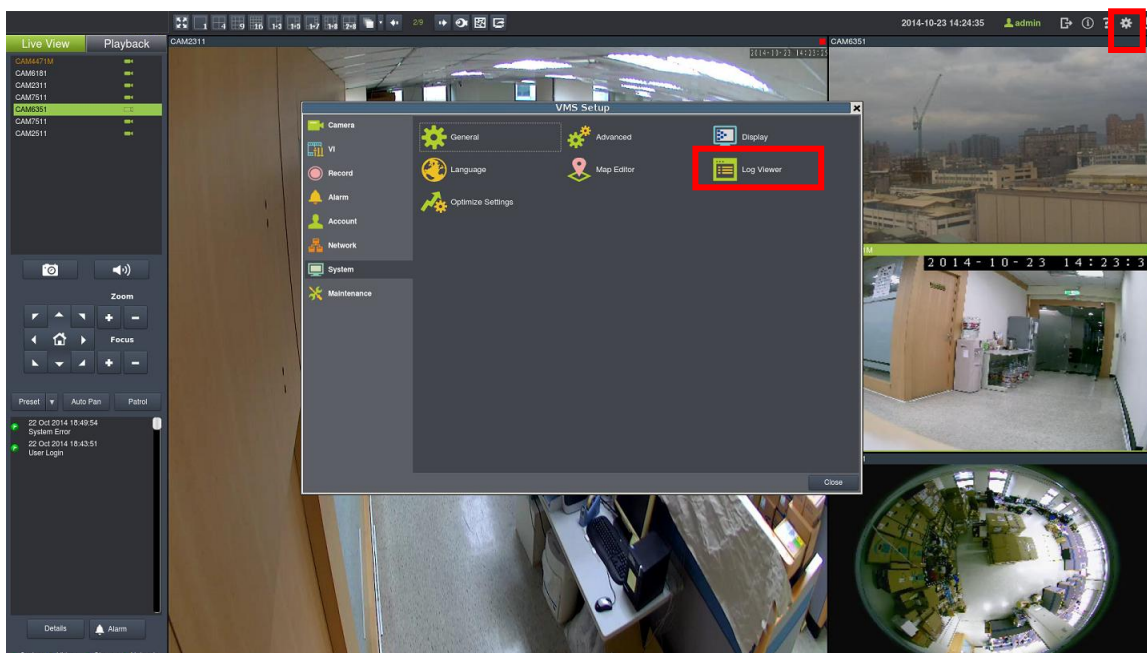
Click the **OK** button to apply the changes and exit the menu.

9.2. Event Log

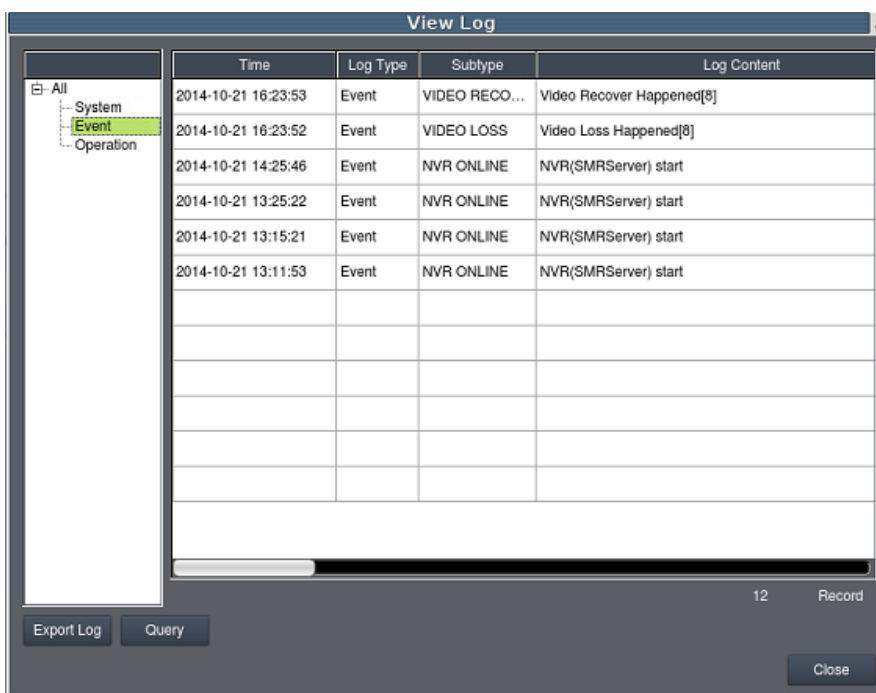
The event log is a comprehensive repository of all the events that occur on the system. To access the event log after logging into the system, right-click the Camera List area and select the **Log Viewer** entry. The *Log Viewer* window will display, click on the **Details** button to see the View Log window.



Or click  to bring out **VMS Setup** window and select **System > Log Viewer**. The *Log Viewer* window will display.



The view log splits into three types, System, concerning with individual modules, Event, concerning with cameras and Operation, concerning with users.



9.2.1. Exporting a Log

If log entries exist, they may be exported by clicking on the **Export Log** button at the bottom of the View Log screen. This will open a dialog box, which prompts users to choose a location, and fill in a name for the saved log. Fill out the location and filename information and click **OK** to save the log file.

9.2.2. Searching the Event Log

Within the View Log screen, click the **Query** button to bring out the Query Log dialog box.

The image shows a 'Query Log' dialog box. At the top, there are three checked checkboxes: 'System', 'Event Type', and 'Operation'. Each checkbox is followed by a dropdown menu currently set to 'ALL'. To the right of these are three more dropdown menus labeled 'Module Name', 'Device Name', and 'Username', all also set to 'ALL'. Below these is a section titled 'Select Log'. It contains two rows of time selection. The first row is labeled 'Start Time' and has a date dropdown set to '10-23-2014', followed by 'Hour' and 'Minute' dropdowns both set to '00'. The second row is labeled 'To' and has a date dropdown set to '10-23-2014', followed by 'Hour' and 'Minute' dropdowns both set to '00'. To the right of the 'To' row are two radio buttons: 'Date Only' (which is selected) and 'Select Time'. At the bottom right of the dialog are two buttons: 'Query' and 'Cancel'.

Within this dialog, users may choose to narrow the search to the three major event types by selecting the checkbox beside the event type:

System

These are errors that occur within individual system modules. In the corresponding selection box, the user can specify a severity (debug, warning, error and fatal in increasing severity) of the event. The user may also choose to search all of the severities.

Event Type

These include errors that occur with cameras. Events include motion detection, video loss, sensor input, clock alarm, disk error and RAID failure. The user may also choose to search over all these types.

Operation

These events include the console startup and stop, system usage, and other events that occur during system operation.

Module Name

The corresponding subfield for *System Type* is *Module Name*. In this selection box, the user can specify a module to search for errors on. The user may also choose to search over all modules by choosing **All**.

Device Name

This subfield contains a list of all the cameras installed on the system. The events can be further narrowed to focus on a single camera by choosing it, or the search can be done over all cameras by choosing **All**.

User Name

Using the *User Name* subfield a search can be narrowed down to an individual user. This selection list contains all the users configured on the system. All the users can be included by selecting **All**.

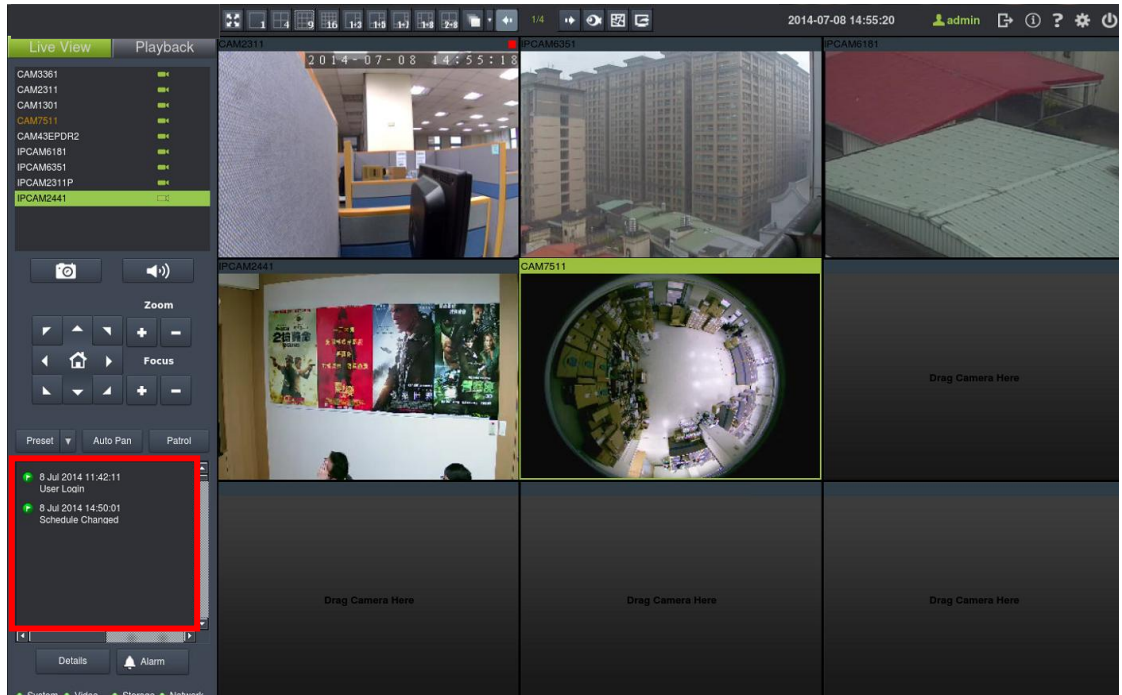
Performing a Search

To perform a search of the log files:

1. If desired, narrow the search by selecting an event type and subfield to search over. More than one event type can be searched.
2. Choose a start date and an end date to search over using the calendar drop-downs.
3. If desired, click **Select time** and select an hour and minute for the start and end times to further narrow the search.
4. Click the **Query** button. The results will show in the main *View Log Screen*.

9.2.3. System Alarm View

The event log will also be displayed on the left corner of the Live View page.



Chapter 10 Search and Playback

In many cases, such as investigations or for reference purposes, it may be useful to be able to replay video streams. The Server has the ability to store video from the IP cameras, as well as playback and export this video information.

10.1. Introduction

Note: You must be logged into a server to access playback functionality.

Click on the *Playback* tab in the live view screen.

The VMS has 3 distinct playback functions:

- Time Search - Plays back according to a time period specified by the user.
- VI Search - Applies VI functionalities to a recorded video stream.
- Event Search - Searches the video stream for distinct events.

- **Note:** Event Search is recommended rather than VI Search, since VI Search uses more bandwidth.

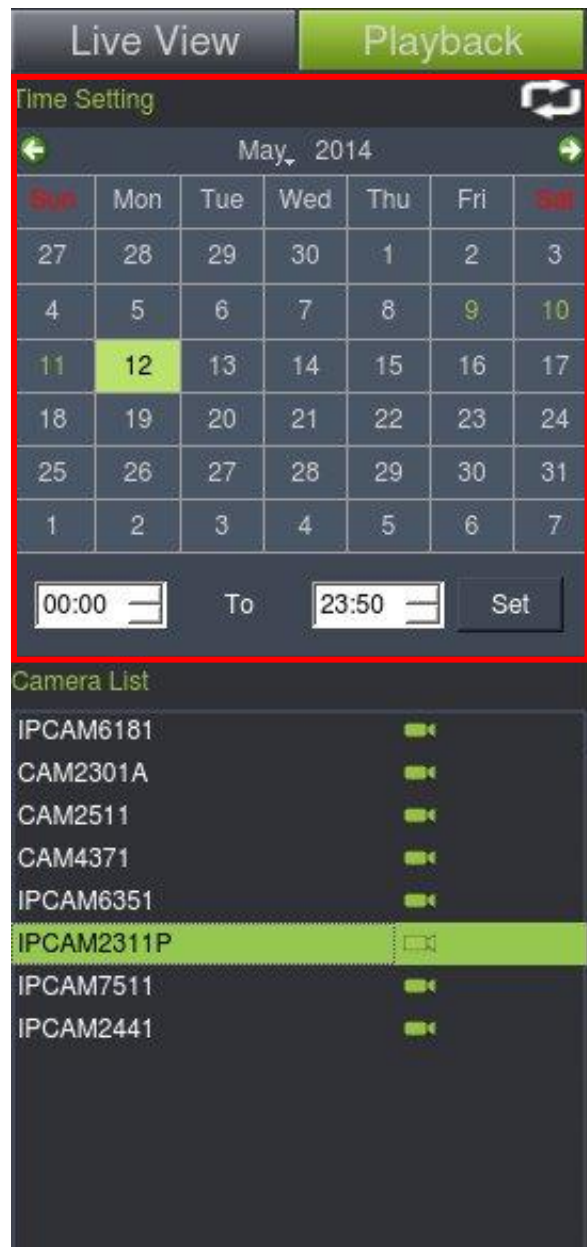


10.2. Time Search

10.2.1. Time Selection

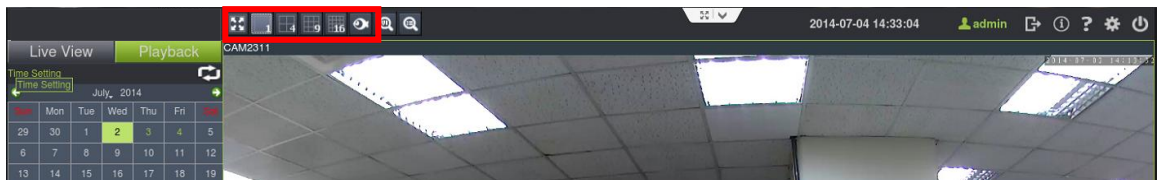
Specified Time

Use the arrows, calendar and time boxes to specify a specific period for search/playback.



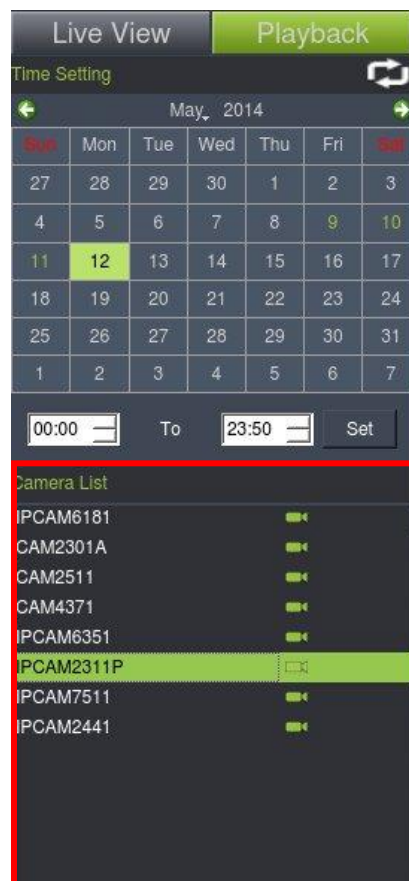
10.2.2. Use of Various Views Selection

Users have the option of viewing the fisheye view or up to 16 recorded video streams at once, or just one stream at a time. Either of these options can be chosen by clicking on corresponding button in the button area above the main view screen. In both cases functionality and operation is the same.



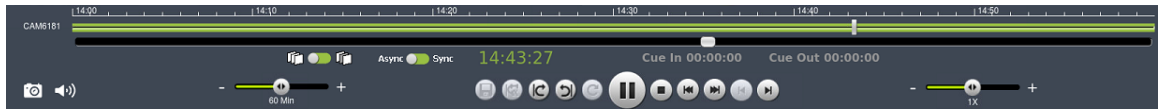
10.2.3. Camera Selection

Once a time period has been selected, the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es).



10.2.4. Timeline

After choosing the cameras to view, the timeline for the camera is displayed below the video window.



The timeline window displays a graphic representation of the video information available for the camera on the date and timeframe you have chosen in the *Select Date* window.

The timeline will, at most, show a period of a little more than 3 hours. If the timeframe that you desire to view is larger than this, the remaining portion of the timeline can be viewed by using the **scrollbar** located beneath the timeline.



The amount of time displayed in the timeline can also be adjusted using the **slider** located next to the scrollbar. Sliding the indicator toward the right will cause a smaller amount of time to be displayed along the length of the timeline.

10.2.5. Playback

Once a timeline has been loaded, you may choose the point to begin playback. This is done by clicking the **timeline**. After selecting the start point you may start playback.















To start playback of a camera's video feed, ensure that the video is selected. Select feeds by clicking the corresponding pane, timeline, or camera name. Once you have selected a camera, you may use the buttons to control the playback. Playback time is denoted above the control buttons.










Note: The system may take a while to buffer the video before playback starts. A status line above the timeline will indicate portions that have been buffered. Jumping to unbuffered points in the video will cause the system to display an error message.

Clicking on a selected portion of the timeline will cause playback to jump to the point that you have clicked on. You must start playback separately for each feed you wish to view.

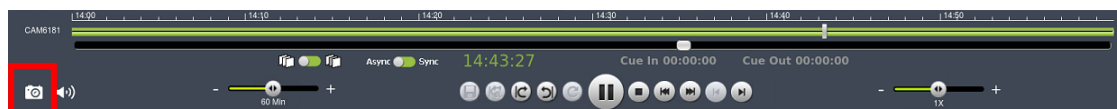
The following table explains the buttons:

	Sync all the views to play videos from the same period of time. While in the Sync mode, the view cannot be changed. Async, undo syn, different views can be selected.
	Snapshot
	Audio volume
	Time range can be set when viewing the playback.
	Full frame mode
	Key frame mode
	Saves video clips/Exports selected clips
	Clear all the Cue-Ins and Cue-Outs
	Set Cue-In marker for clip start
	Set Cue-In marker for clip end
	Automatic reply the clip. (From Cue-in to Cue-Out)
	Starts video playback

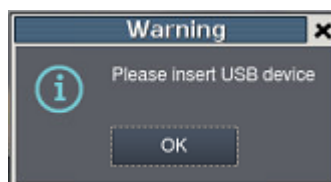
	Pause video playback
	Stops video playback.
	Jumps to the previous frame
	Jumps to the next frame
	Jumps to the previous segment
	Jumps to the next segment
	The play speed can be adjusted from 1x to 8x.

Capturing Screenshot

1. Click the **Snapshot** button located in the button area.



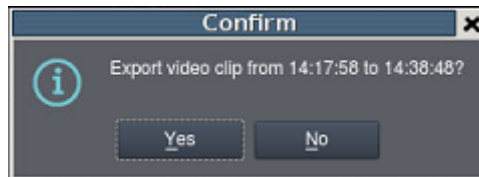
The snapshot will be stored in the USB device. Please have your USB device ready.



Capturing Video Clip

1. Make sure that the video clip is playing.
2. When the beginning of the segment to be captured is reached, click the **Cue In** button.

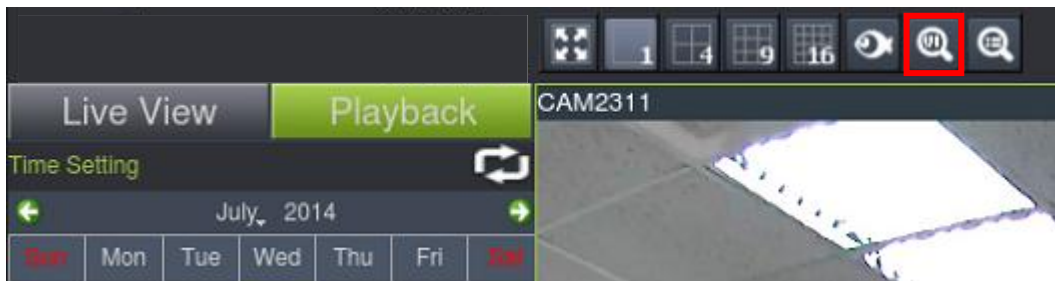
3. When the end of the segment to be captured is reached, click the **Cue Out** button.
4. A popup window will appear for confirmation.



5. Click **Yes** when confirmed. Click **No** and redefine the Cue-In and Cue-Out.
6. The video will be stored in the USB device. Please have your USB device ready.

10.3. VI Search

A VI search involves applying VI to existing recorded video in order to locate a specific event or action. To access the VI search, click the *VI icon* next to the fisheye icon in the button area.



10.3.1. Creating a VI Search

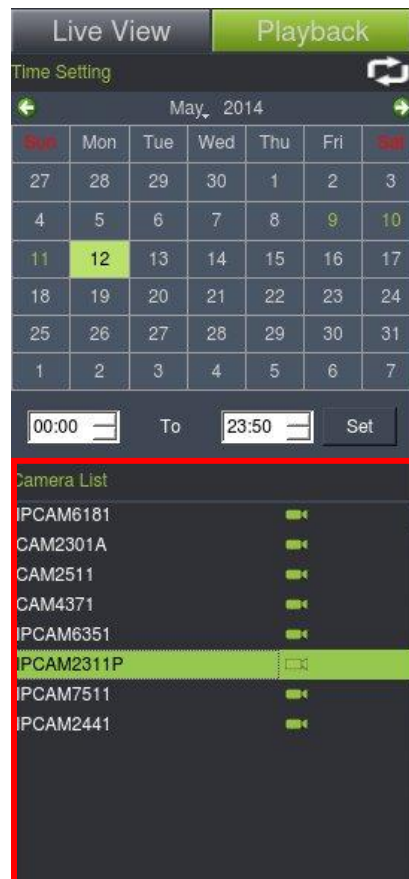
Time Selection

Use the arrows, calendar and time boxes to specify a specific period for search/playback. Once a date is selected, clicking on the boxes will allow you to specify a specific period to search/playback in 10 minute increments.



Camera Selection

Once a time period has been selected, the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es).



Select a camera to perform the VI search on by clicking its entry. This will display an initial thumbnail of the camera output.

Setting New Search Criteria

To create a New VI search, follow directions in the following sections to set up the VI search.

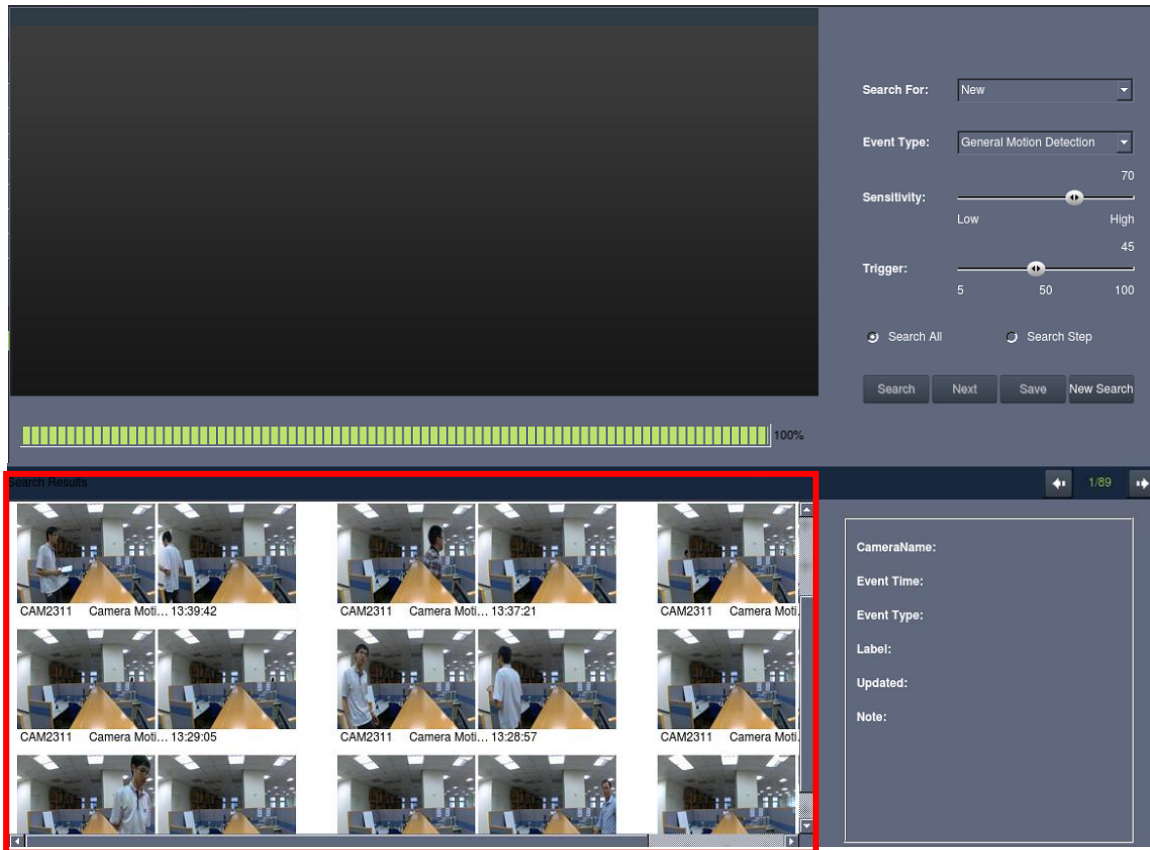
The image shows a software interface for setting search criteria. It has a dark blue background. At the top, there's a 'Search For:' dropdown menu with 'New' selected. Below it is an 'Event Type:' dropdown menu with 'General Motion Detection' selected. Then there are two sliders: 'Sensitivity' with a range from 'Low' to 'High' and a value of 70, and 'Trigger' with a range from 5 to 100 and a value of 45. At the bottom, there are two radio buttons: 'Search All' (which is selected) and 'Search Step'. At the very bottom, there are four buttons: 'Search', 'Next', 'Save', and 'New Search'.

1. **New** in the playback control.
2. Select an **Event Type**.
3. Define the **Sensitivity** and the **Trigger**.
4. **Search Type**
 - **Search All** - Finds all events within the search range that trigger the VI set up.
 - **Search Step** - Finds the first event that triggers the VI, then stops. The next event can be found by repeating the same search.
5. Click **Search** to begin the VI Search.
6. Click **Save** to save the VI search. The system will prompt you for a name. Saved VI searches can also be retrieved using the **Search for** dropdown or by clicking the **Next** button.
7. Click **New Search**, when there are more searches to do.

10.3.2. Using the Search Results

Selecting the Result

Search result thumbnail(s) will be displayed in the results box.



Clicking the thumbnail will select the detection instance. The following information fields are available for each instance:
















- **Camera Name** - The camera used to capture the video.
- **Event Time** - The time the event occurred.
- **Event Type** - The type of VI detection that the event triggered.
- **Label** - A user-defined label (optional).
- **Updated** - The last time the event was updated.





Result Playback

Once a result is selected by clicking on it, playback can be started by double clicking on the thumbnail. Alternatively, you may right-click the thumbnail and click **Play**. A ten

minute clip containing the event will begin playing, with the start time synchronized with the start of the event.

The following functions are available for playback:

	Sync all the views to play videos from the same period of time. While in the Sync mode, the view cannot be changed. Async, undo syn, different views can be selected.
	Snapshot
	Audio volume
	Time range can be set when viewing the playback.
	Full frame mode
	Key frame mode
	Saves video clips/Exports selected clips
	Clear all the Cue-Ins and Cue-Outs
	Set Cue-In marker for clip start
	Set Cue-In marker for clip end
	Automatic reply the clip. (From Cue-in to Cue-Out)
	Starts video playback
	Pause video playback
	Stops video playback.
	Jumps to the previous frame

	Jumps to the next frame
	Jumps to the previous segment
	Jumps to the next segment
	The play speed can be adjusted from 1x to 8x.

10.4. Event Search

An Event search involves searching for multiple tagged events over one more cameras. To access the Event search, click the *Event Search icon* next to the VI Search icon in the button area.



10.4.1. Creating an Event Search

Time Selection

Use the arrows, calendar and time boxes to specify a specific period for search/playback. Once a date is selected, clicking on the boxes will allow you to specify a specific period to search/playback in 10 minute increments.



Camera Selection

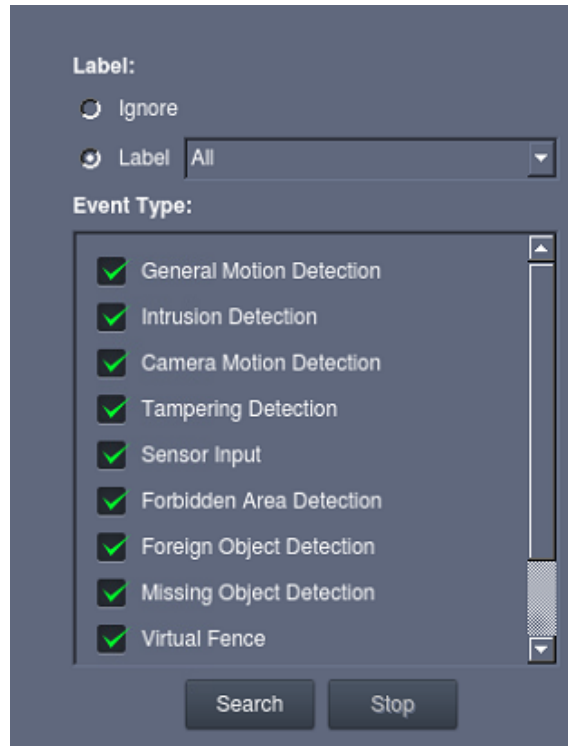
Once a time period has been selected, the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es).



Select a camera to perform the Event search on by clicking its entry. This will display an initial thumbnail of the camera output.

Setting Event Search Criteria

1. Selecting **Ignore** will search for all labels. Choose an **Event Type** and/or a **Label** to search for.



The image shows a software interface for setting event search criteria. It has a dark grey background. At the top, under the heading "Label:", there are two radio buttons. The first is labeled "Ignore" and is selected. The second is labeled "Label" and is not selected. To the right of the "Label" radio button is a dropdown menu currently showing "All". Below this, under the heading "Event Type:", there is a list of ten event types, each preceded by a green checkmark in a box. The event types are: General Motion Detection, Intrusion Detection, Camera Motion Detection, Tampering Detection, Sensor Input, Forbidden Area Detection, Foreign Object Detection, Missing Object Detection, and Virtual Fence. At the bottom of the dialog are two buttons: "Search" and "Stop".

Label:

☒ Ignore

☐ Label All

Event Type:

- ☒ General Motion Detection
- ☒ Intrusion Detection
- ☒ Camera Motion Detection
- ☒ Tampering Detection
- ☒ Sensor Input
- ☒ Forbidden Area Detection
- ☒ Foreign Object Detection
- ☒ Missing Object Detection
- ☒ Virtual Fence

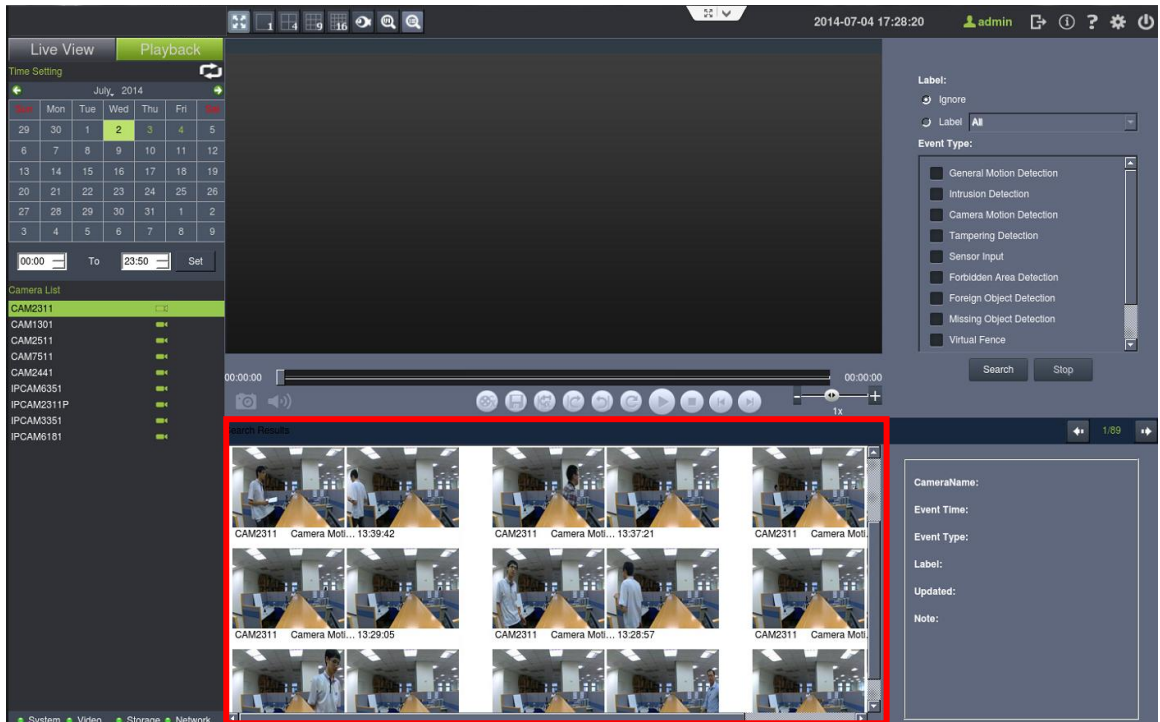
Search Stop

2. Click **Search** to begin the search. Results will display in the *Search Results* panel.

10.4.2. Using the Search Results

Selecting the Result

Search result thumbnail(s) will be displayed in the results box.



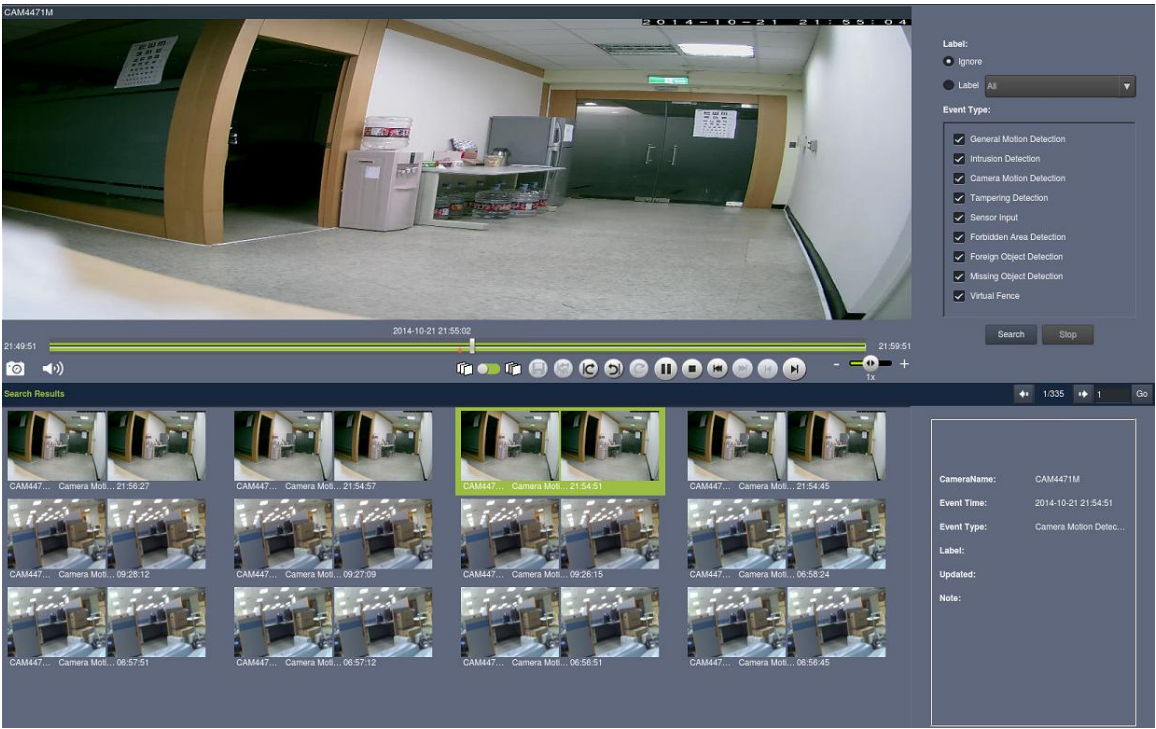
- **Camera Name** - The camera used to capture the video.
- **Event Time** - The time the event occurred.
- **Event Type** - The type of VI detection (if any) that the event triggered (optional).
- **Label** - A user-defined label (optional).
- **Updated** - The last time the event was updated.

Result Playback



Once a result is selected by clicking on it, playback can be started by double clicking on the thumbnail. Alternatively, you may right-click the thumbnail and click **Play**. A ten minute clip containing the event will begin playing, with the start time synchronized with the start of the event.

















Synchronize Playback can show you results of different cameras in the same period of time via dragging the cameras you'd like to compare to the view area.

Label can be added as Mark, Check, Clear and Suspicious.




The following functions are available for playback:

	<p>Sync all the views to play videos from the same period of time. While in the Sync mode, the view cannot be changed.</p> <p>Async, undo syn, different views can be selected.</p>
	<p>Snapshot</p>

	Audio volume
	Time range can be set when viewing the playback.
	Full frame mode
	Key frame mode
	Saves video clips/Exports selected clips
	Clear all the Cue-Ins and Cue-Outs
	Set Cue-In marker for clip start
	Set Cue-In marker for clip end
	Automatic reply the clip. (From Cue-in to Cue-Out)
	Starts video playback
	Pause video playback
	Stops video playback.
	Jumps to the previous frame
	Jumps to the next frame
	Jumps to the previous segment
	Jumps to the next segment
	The play speed can be adjusted from 1x to 8x.

Chapter 11. VMS Setup

11.1. Camera

Click  to bring out **VMS Setup** window and select **Camera** to set the camera related settings.



11.1.1. Edit Camera

The Edit Camera allows you to configure camera settings such as camera vendor, model and permission to access the cameras. See Chapter 8.2.2. *Edit Camera* for more details.

11.1.2. Advanced Camera

Advanced Camera allows you to configure the encoding method, resolution, maximum frame filter and the quality. See Chapter 8.3.2 *Advanced Video Settings* for more details.

11.1.3. General Camera Settings

General Camera allows you to configure the camera connection. See Chapter 8.2.1 *General Camera Settings* for more details.

11.1.4. Image Settings

Image allows you to configure the camera image quality. See Chapter 8.3.1 *Camera Image Settings* for more details.

11.1.5. PTZ Camera Settings

PTZ allows you to configure the PTZ cameras. See Chapter 8.5 *PTZ Setup* for more details.

11.1.6. PTZ Preset Settings

Preset allows you to configure the PTZ presets. See Chapter 8.5.2 *PTZ Preset Settings* for more details.

11.1.7. PTZ Patrol Settings

Patrol allows you to configure the PTZ patrol. See Chapter 8.5.3 *PTZ Patrol Settings* for more details.

11.1.8. OSD Settings

OSD allows you to configure the OSD overlay, such as camera name, date, time to show on the view. See Chapter 8.2.3 *OSD Settings* for more details.


11.1.9. Mask Settings

Mask allows you to configure the privacy mask settings. See Chapter 8.2.4 *Privacy Mask Settings* for more details.

11.1.10. Optimize Settings

Optimize allows you to configure the camera to the default settings. See Chapter 8.5.4 Optimize a Camera for more details.

11.2. VI

Click  to bring out **VMS Setup** window and select **VI** to set the VI related settings.



11.2.1. Camera Motion Detection

Camera motion detection involves using the camera hardware to analyze the video feed and detect motion in specified areas. See Chapter 8.4.1. *Camera Motion Detection* for more details.

11.2.2. General Motion Detection

Automatically detect the moving target entering the security area. When it moves, an alarm will be triggered. See Chapter 8.4.2 *General Motion Detection* for more details.

11.2.3. Tampering Detection

Tampering detection involves using the software to determine when the camera has been improperly moved or redirected. See Chapter 8.4.3 *Tampering Detection* for more details.

11.2.4. Forbidden Area Detection

Forbidden area detection involves using the software to analyze the video feed and immediately detect any object in specified areas. See Chapter 8.4.4 *Forbidden Area Detection* for more details.

11.2.5. Intrusion Detection

Intrusion detection involves using the software to analyze the video feed and detect intrusion larger than a certain size. See Chapter 8.4.5 *Intrusion Detection* for more details.

11.2.6. Virtual Fence Detection

Virtual fence involves using the software to create a fence-crossing detection of the demanding object. See Chapter 8.4.6 *Virtual Fence Detection* for more details.

11.2.7. Missing Object Detection

Missing object detection involves using the software to analyze the video feed and detect missing objects larger than a certain size. See Chapter 8.4.7 *Missing Object Detection* for more details.

11.2.8. Foreign Object Detection

Foreign object detection involves using the software to analyze a video feed and detect objects that do not belong. See Chapter 8.4.8 *Virtual Foreign Object Detection* for more details.

11.2.9. Tailgating Detection

Tailgating detection involves using the software to analyze the video feed and detect a tailgating object crossing over the restricted area. See Chapter 8.4.9 *Tailgating Detection* for more details.


11.2.10. Go In/Out Detection

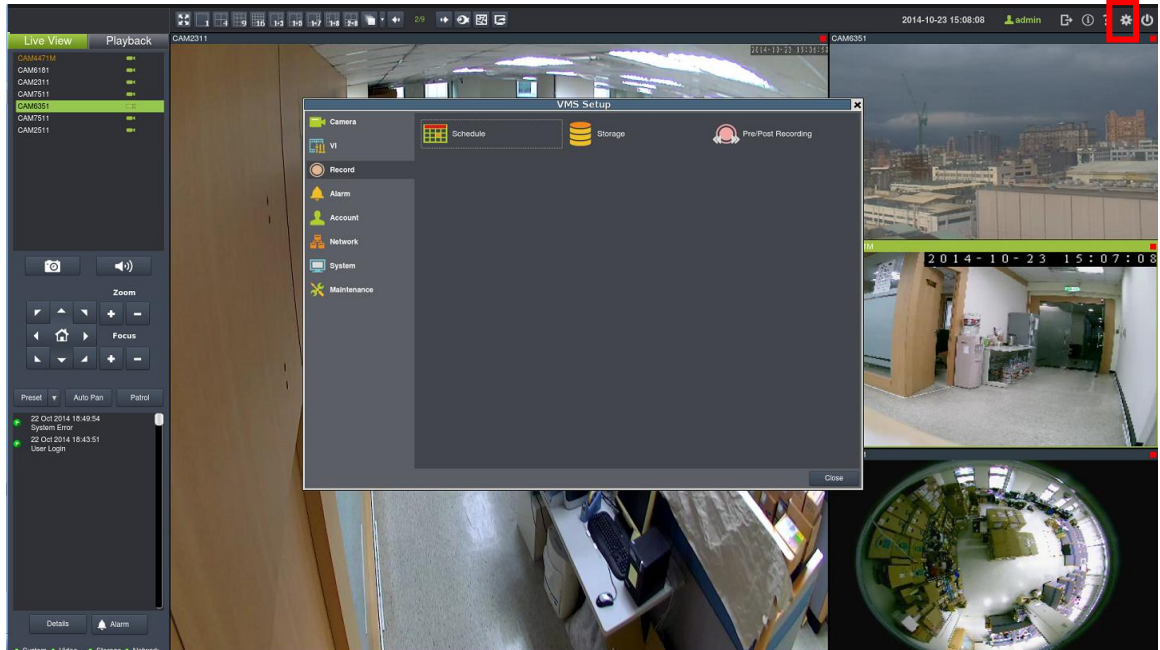
Go In/Out detection involves using the software to analyze the video feed and detect a go in/out object crossing over the restricted area. See Chapter 8.4.10 *Go In/Out Detection* for more details.

11.2.11. General Setting

General Settings involves setting the frame interval. It takes less system resources for bigger trigger frame intervals but the accuracy will be lower.

11.3. Recording

Click  to bring out **VMS Setup** window and select **Record** to set the recording related settings.



11.3.1. Schedule

A Recording Schedule can be created to apply to an entire Server. See Chapter 7.1.4 *Recording Schedule* for more details.


11.3.2. Storage

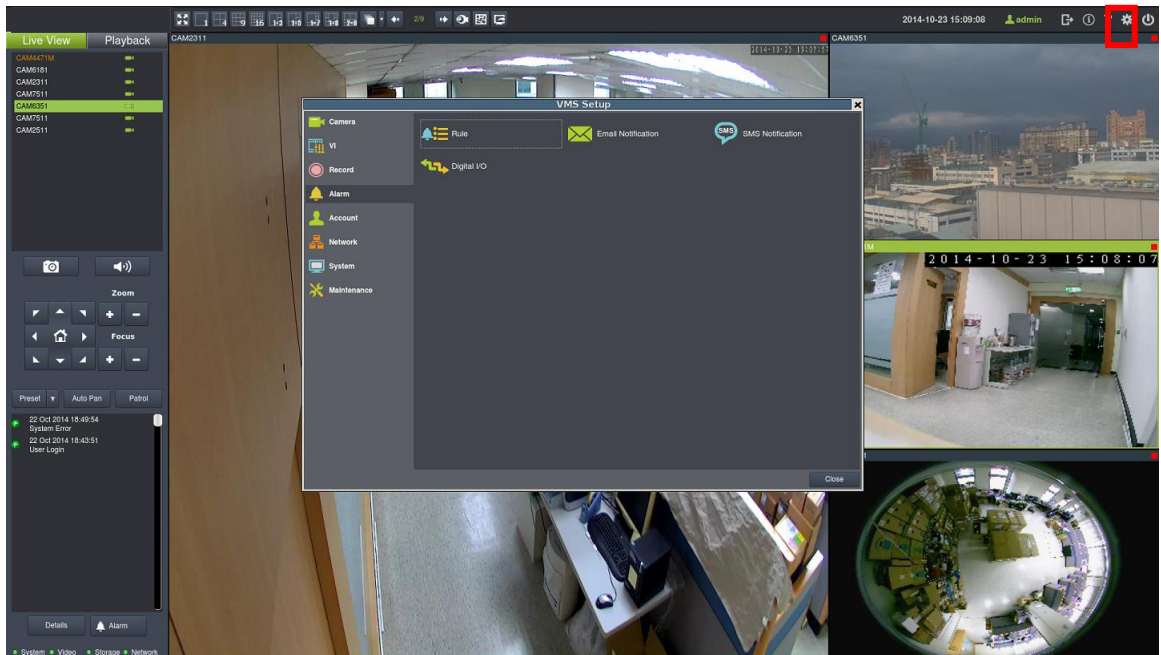
Opens the Storage Manager that allows you to configure storage settings. See Chapter 7.1.3. *Storage Management* for more details.

11.3.3. Pre/Post Recording

The Server can trace back and preserve video/images from several minutes before and after the occurrence of an alarm. See Chapter 7.1.5 *Pre/Post Recording* for more details.

11.4. Alarm

Click  to bring out **VMS Setup** window and select **Alarm** to set the alarm related settings.



11.4.1. Alarm Rules

In the Alarm Rules, you can combine the alarm trigger conditions with action items such as event notification, video recording, and/or camera movements. See Chapter 9.1. *Alarm Rules* for more details.

11.4.2. Email

When the alarm is triggered, an E-Mail will be sent. See Chapter 9.1.1. *Adding an Alarm Rule* for more details.

11.4.3. SMS

Configures the SMS setting. See Chapter 9.1.1. *Adding an Alarm Rule* for more details.

11.4.4. Digital I/O Settings

Allows you to configure digital I/O port settings.

Digital I/O Settings

Camera ListCAM4471M

Camera Port	Name	Status	Current Status
DI0	input0	Off	High
DO1	output0	Off	High

Digital Output Simulation

1


Digital Input Monitor

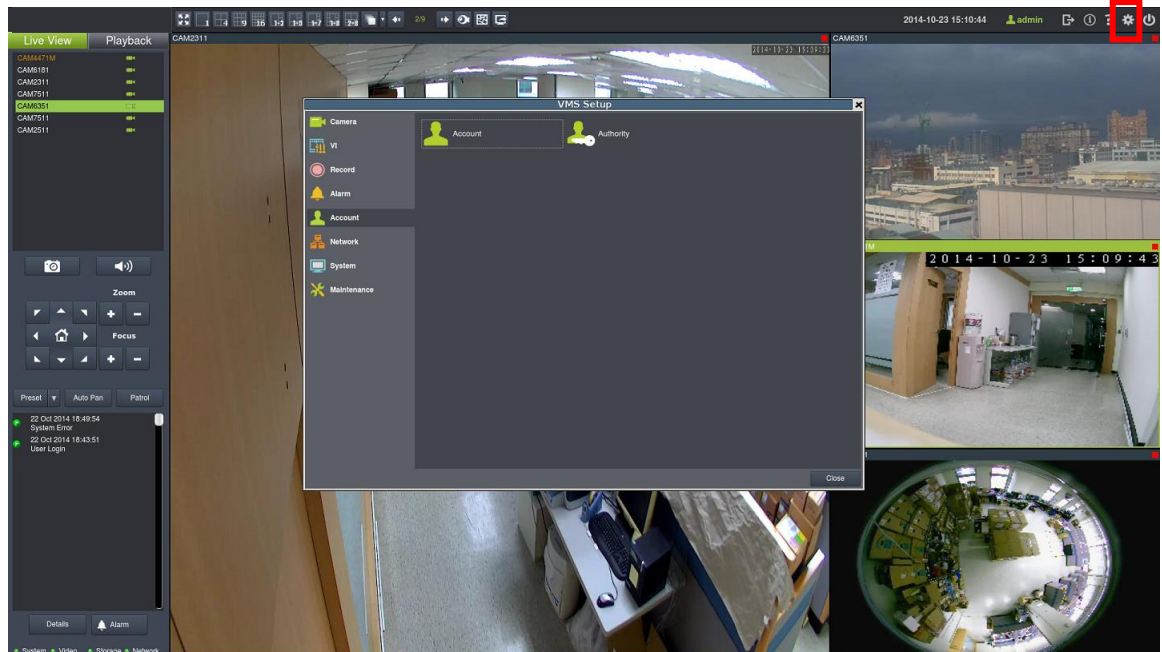
0

OK

Cancel

11.5. Account

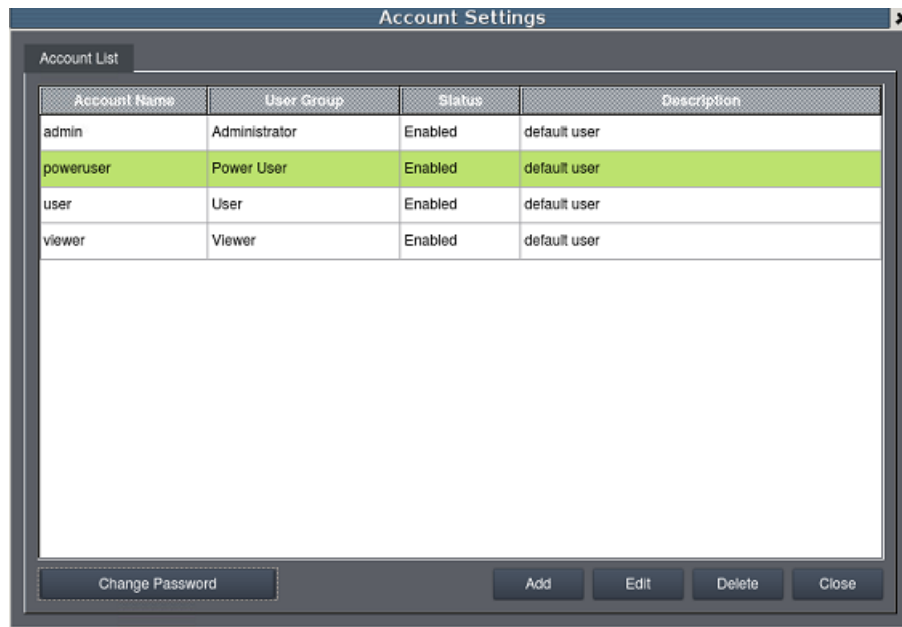
Click  to bring out **VMS Setup** window and select **Account** to set the account related settings. In this session, accounts and their authorities can be edited, added, and deleted.



11.5.1. Accounts

The *Account List* provides the following information about each account:

- **Account Name**
- **User Group** - Type for this user.
- **Status** - This shows if the user is disabled or enabled.
- **Description** - A simple description of the user.

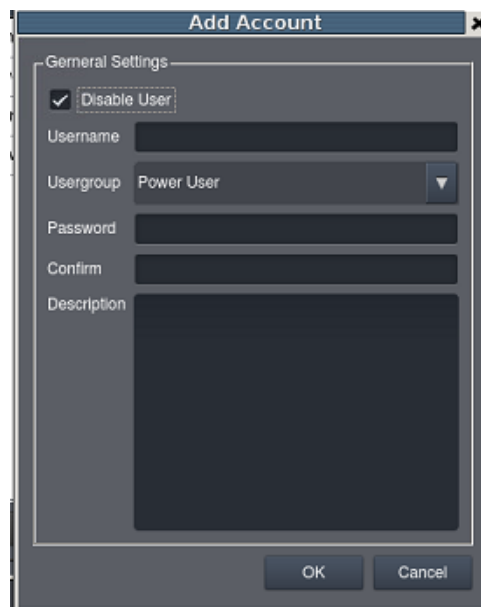


The screenshot shows a window titled "Account Settings" with a tab labeled "Account List". Inside the window is a table with four columns: "Account Name", "User Group", "Status", and "Description". The table contains four rows of user accounts. The "poweruser" row is highlighted in green. Below the table, there is a "Change Password" button and a row of four buttons: "Add", "Edit", "Delete", and "Close".

Account Name	User Group	Status	Description
admin	Administrator	Enabled	default user
poweruser	Power User	Enabled	default user
user	User	Enabled	default user
viewer	Viewer	Enabled	default user

Add Account

To add an account to the domain:



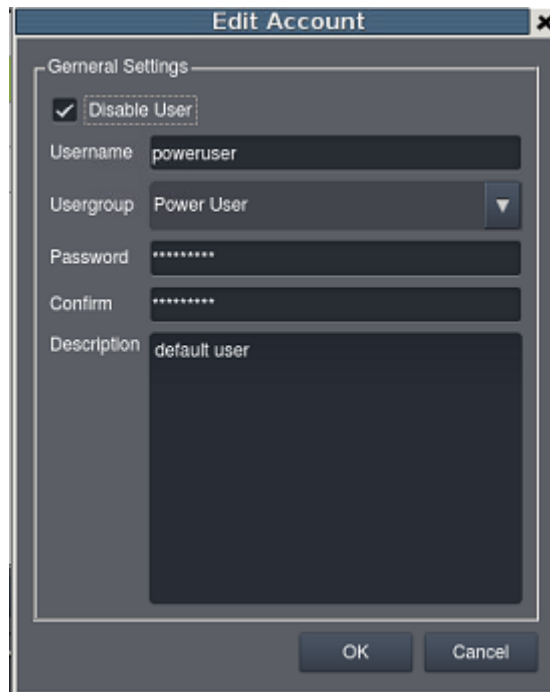
The screenshot shows a dialog box titled "Add Account". It has a "General Settings" section with a "Disable User" checkbox that is checked. Below this are fields for "Username", "Usergroup" (a dropdown menu currently showing "Power User"), "Password", "Confirm", and "Description" (a text area). At the bottom are "OK" and "Cancel" buttons.

1. Click the **Add** button at the bottom of the *Account List* screen.
2. In the resulting screen fill out information for the new account:
 - **Username**
 - **User Group** - Select a user type for this user. There are four options:
 - **Administrator** - This group has complete management privileges, including account and VMS/Server management rights.
 - **Power User** - This group has complete account management rights, but does not have many VMS/Server configuration rights.
 - **User** - This group has no configuration rights and limited VMS/Server performance statistics.
 - **Viewer** - This group is limited only to viewing, and has no access to configuration or performance statistics.
 - **Password / Confirm Password** - The password must be typed twice for confirmation purposes.
 - **Description** - A simple description of the new user.
3. Check the **Disable User** box to disable this account.
4. Click **Ok** to add the new account. The account will appear in the *Account List*.

Editing an Account

To edit an account to the domain:

1. Access the *Account List* node in the *VMS Setup*.
2. Select the account that you wish to edit by clicking on the account.



3. Click the **Edit** button at the bottom of the *Account List* screen.
4. In the resulting screen change any of the following account information:
 - **User Group** - Selects a user type for this user. There are four options:
 - **Administrator** - This group has complete management privileges, including account and VMS/SMR Server management rights.
 - **Power User** - This group has complete account management rights, but does not have many VMS/SMR Server configuration rights.
 - **User** - This group has no configuration rights and limited VMS/Server performance statistics.
 - **Viewer** - This group is limited only to viewing, and has no access to configuration or performance statistics.
 - **Password/Confirm Password** - If changed the password must be typed twice for confirmation purposes.
 - **Description** - A simple description of the user.

5. If desired check the **Disable User** box to disable this account.
6. Click **Ok** to save the changes to the account. If the account description, user group or status changes, it will be reflected in the *Account List*.

Changing an Account Password

In addition to editing the password from using the *Account List* editing function, the password for the current account can also be changed by clicking the **Change Password** at the lower left corner of *Account List Window*.

This will display a dialog that allows you to enter and confirm a new password.



Deleting an Account

To delete an account to the domain:


1. Access the *Account List* node in the *VMS Setup*.
2. Select the account that you wish to delete by clicking on the account.
3. Click the **Delete** button at the bottom of the *Account List* screen.
4. When prompted to confirm deletion click **Yes** to delete the account. The deletion will be reflected in the *Account List*.

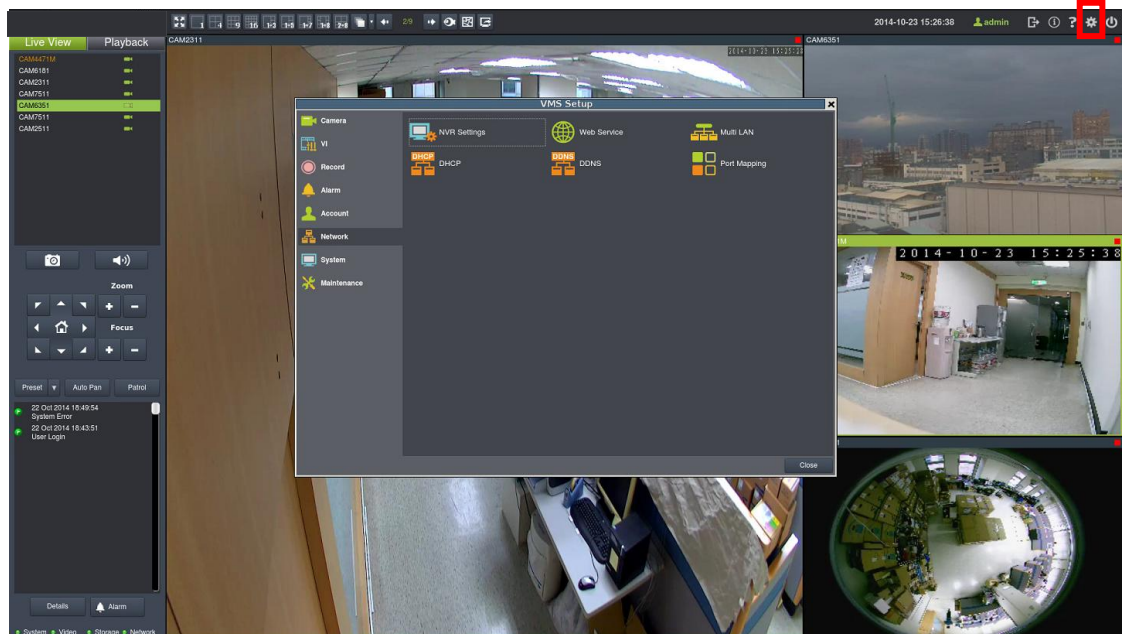
Note: The *Admin* account cannot be deleted.

11.5.2. Account Authority Settings



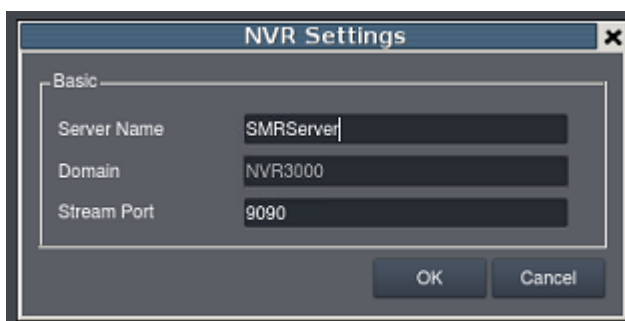
11.6. Network

Click  to bring out **VMS Setup** window and select **Network** to set the network related settings.



11.6.1. NVR Settings

Users can change both the setting of the stream port and the IP address by editing the Server.



11.6.2. Web Server

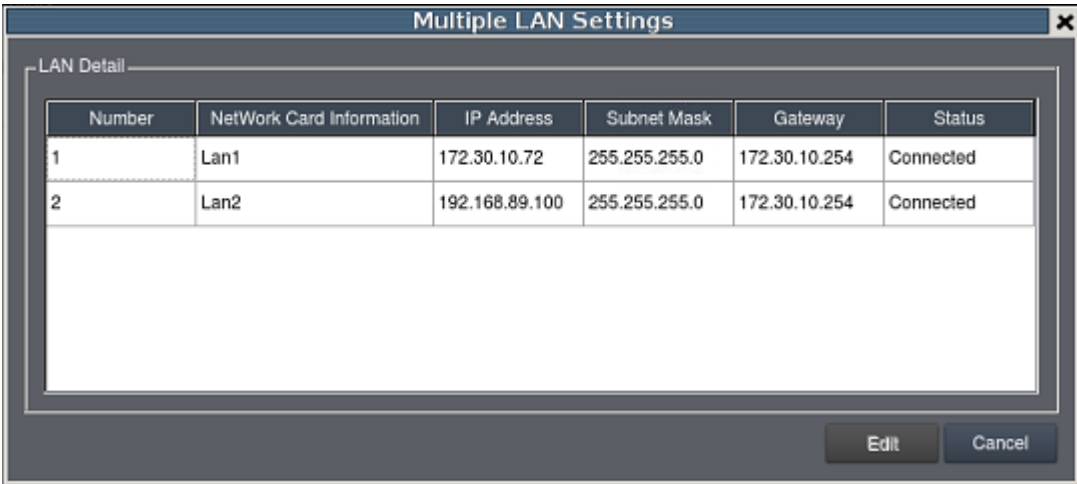
For users who want to use the Web Client/Mobile Client, please fill in the following information for the Web Server settings.



Note: (1) User may just keep the default settings in the Web Server. (2) Do not set the Web Server Port as these port numbers - 8080 (Web Stream Port), 9090 (NVR Stream Port), 2809 (NVR Server Login Port), 7735 (TV Wall Port (2.5.0)), 7734, 1024, 9010 (Domain Broadcast Port), 9030 (Domain Client Message Port), 9040 (Domain Console Message Port), 9050 (Domain Local Communication Port), 9020 (Domain Remote Communication Port), 9080 (Domain Local Log Data Download Port), 9081 (Domain Remote Log Data Download Port), 9060 (Domain Local Data Port), 9061 (Domain Remote Data Port), 15507 (Domain Local Log Message Download Port), 15503 (Domain Remote Log Message Download Port), 15501 (Domain Remote Log Upload port), 15505 (Domain Local Log Upload Port), 40000 (NVR Broadcast Port), 50000 (NVR Message Port).

11.6.3. Multiple LAN

Multiple network cards can be supported. Their information is listed as below:




The "Multiple LAN Settings" dialog box displays a table of LAN details. The table has six columns: Number, NetWork Card Information, IP Address, Subnet Mask, Gateway, and Status. It lists two LANs, both with a status of "Connected".

Number	NetWork Card Information	IP Address	Subnet Mask	Gateway	Status
1	Lan1	172.30.10.72	255.255.255.0	172.30.10.254	Connected
2	Lan2	192.168.89.100	255.255.255.0	172.30.10.254	Connected

Buttons: Edit, Cancel

Click the “Edit” to set the Network Card to DHCP Auto-Configuration or Fixed IP.



The "Network Card Settings" dialog box allows configuration of network settings. It features two radio buttons: "DHCP Auto-Configuration" (selected) and "Fixed IP Address". Below these are input fields for IP Address, Subnet Mask, Gateway, and DNS.

Options:

- ☒ DHCP Auto-Configuration
- ☐ Fixed IP Address

Fields:

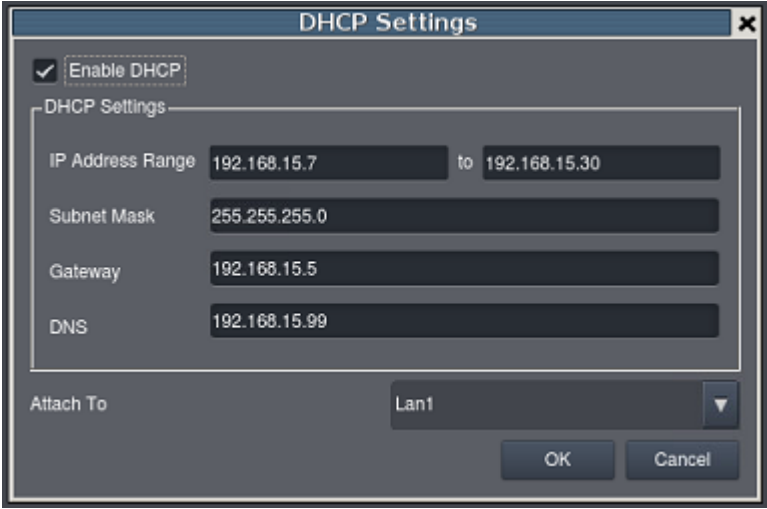
- IP Address: 172.30.10.72
- Subnet Mask: 255.255.255.0
- Gateway: 172.30.10.254
- DNS: 192.168.99.13

Buttons: OK, Cancel

11.6.4. DHCP Settings

The VMS has built in DHCP server functionality. Although this function is disabled by factory default, it should be turned on in the event that there is no DHCP service available. When enabled, the VMS will assume DHCP Server duties and assign addresses within the range specified.

Note: You may skip this step if you have separate DHCP service. Most routing devices will have DHCP capabilities.



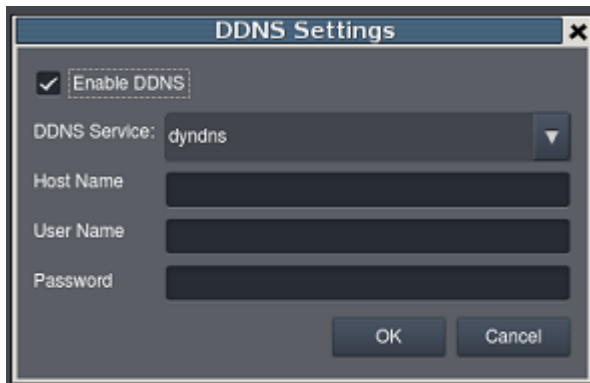
The screenshot shows a 'DHCP Settings' window. At the top, there is a checkbox labeled 'Enable DHCP' which is checked. Below this is a section titled 'DHCP Settings' containing four input fields: 'IP Address Range' with the value '192.168.15.7 to 192.168.15.30', 'Subnet Mask' with '255.255.255.0', 'Gateway' with '192.168.15.5', and 'DNS' with '192.168.15.99'. Below these fields is an 'Attach To' dropdown menu currently showing 'Lan1'. At the bottom right of the window are 'OK' and 'Cancel' buttons.

1. Fill in the following information:

- **IP Address Range** - The range of addresses to be assigned. The first IP address should be lower than the second IP address.
- **Subnet Mask**
- **Router** - The router IP
- **Domain Name** - The DNS IP

Note: The DHCP service should be attached to a network card.

11.6.5. DDNS Setting

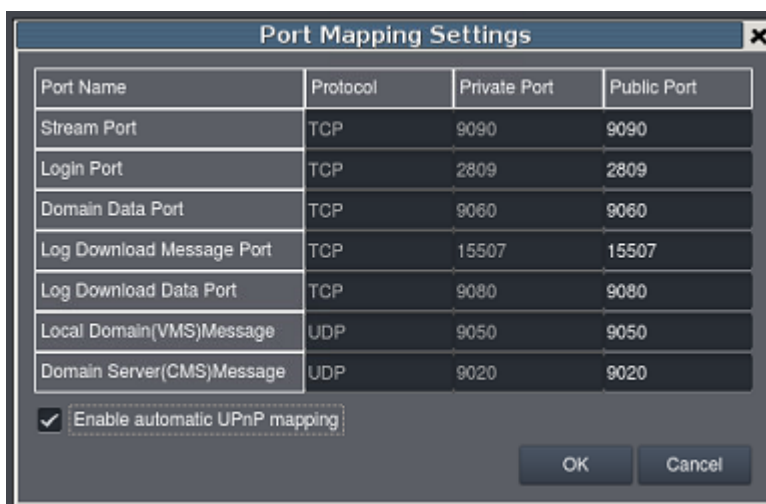


DDNS (Dynamic Domain Name Server) is a protocol that enables the camera to maintain a static connection address, even when its IP changes. Access using this feature is disabled by default.

Connecting using DDNS requires registration on third-party websites for DDNS services. Select desired DDNS service website, check the **Enable DDNS** option, and fill in valid user name and password. You can then access the camera through the registered domain name.

11.6.6. Port Mapping

A *Router Port Mapping* window will prompt for entering port numbers. See Chapter 3.4.1. Port Forwarding for Accessing VMS Server for more details.



Port Name	Protocol	Private Port	Public Port
Stream Port	TCP	9090	9090
Login Port	TCP	2809	2809
Domain Data Port	TCP	9060	9060
Log Download Message Port	TCP	15507	15507
Log Download Data Port	TCP	9080	9080
Local Domain(VMS)Message	UDP	9050	9050
Domain Server(CMS)Message	UDP	9020	9020

Stream Port: 9090

Login: Port: 2809

Doman Data Port: 9060

Log Download Message Port: 15507

Log Download Data Port: 9080

2. Open Ports on the Router

Host Ports: The private ports that the internal VMS/SMR Server use, which are unchangeable.


Global Ports: The public ports for remote clients to connect to the internal VMS/SMR Server. The Global ports are changeable, but the simplest way is to make them the same with the host ports.

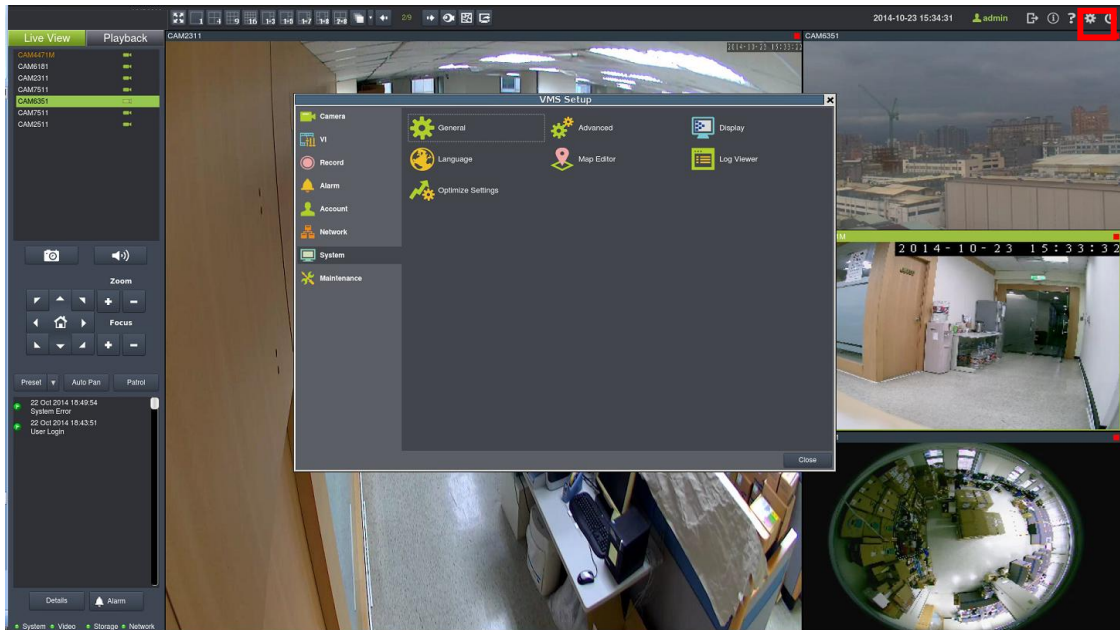
Please open the listed ports on your router:

Port(Host/Global Port)	Protocol	Port Number
Domain Message Port	UDP	9050
Domain Data Port	TCP	9060
Login Port	TCP	2809
Stream Port	TCP	9090
Log Download Message Port	TCP	15507
Log Download Data Port	TCP	9080

Note: Camera port (default: 80) and stream port (default: 6002) for accessing cameras should be opened while VMS/SMR Server and the cameras and are not in the same LAN.

11.7. System

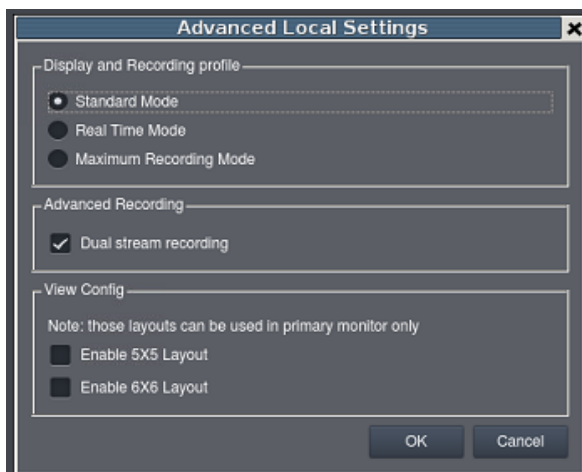
Click  to bring out **VMS Setup** window and select **System** to set the system related settings.



11.7.1. General

Server settings can be configured under the *General Server Settings* menu. See Chapter 7.1.1. *General Server Settings* for more details.

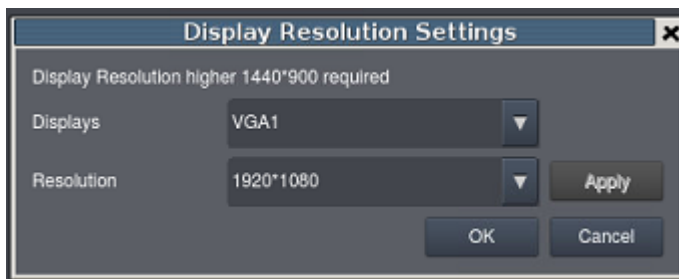
11.7.2. Advanced



Settings concerning display and recording profile, dual stream recording, and view layout can be configured here.

11.7.3. Display Resolution Settings

Shows the monitor resolution, and allows you to change its setting.



11.7.4. Language

The system supports the following languages: Dutch, English, German, Italian, Japanese, Korean, Persian, Russian, Simplified Chinese, Spanish, Traditional Chinese, and Turkish.



11.7.5. Map Editor

E-map can be configured here. See Chapter 6.2.1. E-map for more details.

11.7.6. Log Viewer


Log can be viewed under the View Log menu. See Chapter 9.2. *Event Log* for more details.

11.7.7. Optimize Settings

Once click on the option “Optimize now”, a confirm window will pop up. This action will apply to all cameras connected.



11.8. Maintenance

Click  to bring out **VMS Setup** window and select **Maintenance** to set the maintenance related settings.



11.8.1. Stream Status

From here you can see all the stream information, such as channel, camera name, codec, resolution, FPS, and bit-rate.

Stream Status									
Channel	Camera name	S1.Codec	S1.Resolution	S1.FPS	S1.BitRate	S2.Codec	S2.Resolution	S2.FPS	S2.BitRate
0	CAM2311	H.264	1920X1080	15	3.9Mbps	H.264	320X240	15	0.5Mbps
1	CAM4471M	H.264	2048X1536	20	5.7Mbps	H.264	320X240	30	0.5Mbps
2	CAM7511	H.264	2560X1920	10	5.0Mbps	H.264	320X240	10	0.5Mbps
3	CAM6181	H.264	720X480	60	2.0Mbps	H.264	352X240	30	0.2Mbps

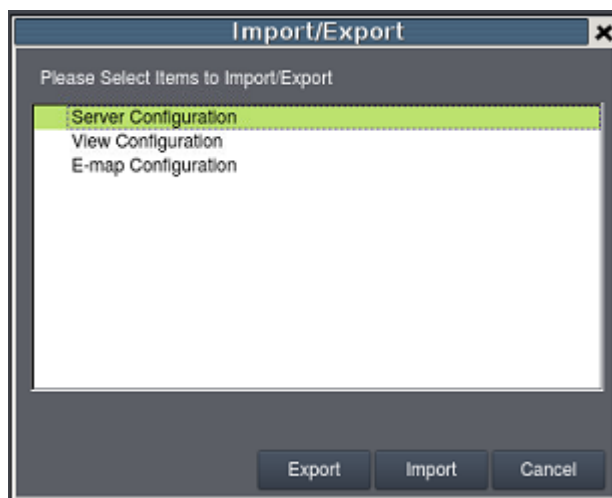
11.8.2. Upgrade

Upgrading can be done here. Have the USB with the upgrade patch file connected to the system. And then click the Rescan button. The upgrade patch file in the USB will be read and the upgrading can begin.

Once the upgrade is done, the system will reboot to update the settings.



11.8.3. Import/Export



The following types of configuration/setup files can be imported/exported to the Server:

- **Server Configuration**
- **View Configuration**
- **E-map File**

Importing Parameters

To import parameters into the Server:

1. Select the item that you wish to import by clicking on the item type.
2. Click the **Import** button. A windows explorer dialog will appear.
3. Select the file to import from the file explorer, and click **Open** to import the file.
4. Click **OK** to confirm import. The Server will require a restart before imported configurations and files are applied.

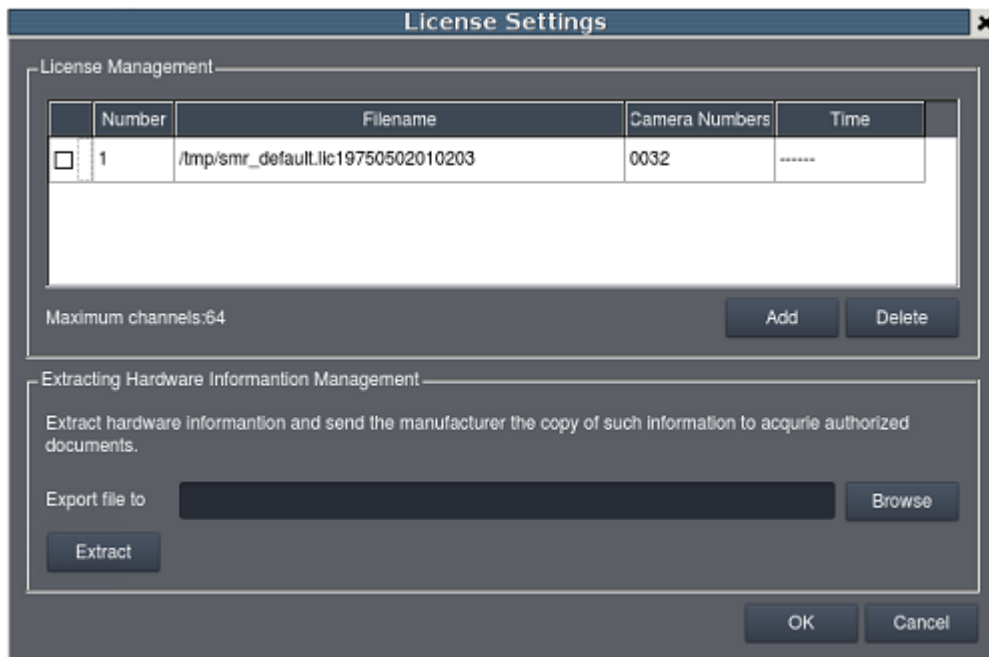
Exporting Parameters

To export parameters into the Server:

1. Select the item that you wish to export by clicking on the item type.
2. Click the **Export** button. A windows explorer dialog will appear.
3. Input a filename and select the export path in the file explorer, and click **Save** to export the file.

11.8.4. License

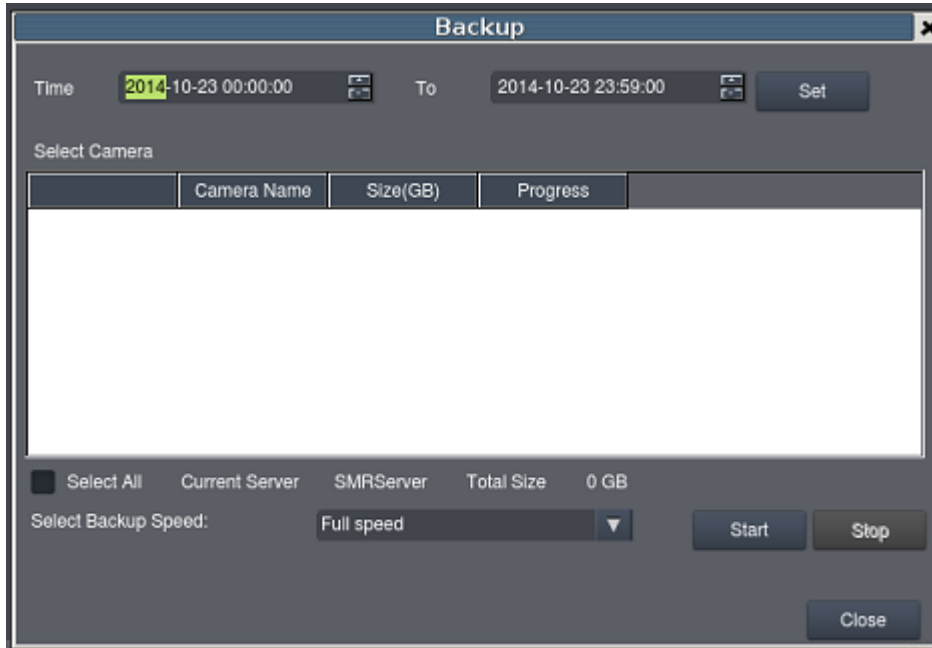
Extra supported channels can be added by purchasing licenses.



1. Click **Browse** under Information Storage Address, and enter a file name for exporting the existing channel information.
2. Click **Extract**. The *.info file will be stored to the selected path or to the default path usually your desktop.
3. Provide the extracted file to your distributors or dealers to acquire the license information. And they will return the license file ("License Key+Channel Number.lis") for you to add the channels.
4. After receiving the license file, go back to the system Local Client Console under setting and click ADD to upload your "xxx.lis" file from the online registration to the VMS add-on channels (License).
5. Check the License Management to make sure if the channels are added successfully. Once your purchased channels are added on, click "OK" to confirm and leave this page.

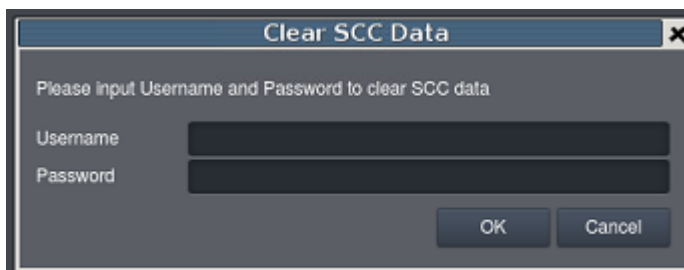
11.8.5. System Backup

The video recording can be backed up. Set the time, select the camera, and choose the saving path for the backup files.



11.8.6. Clear SCC Data

Allows you to clear the SCC /VMS data on the Domain Server.



11.8.7. Remote Assistant

This functionality can be used for the technician to have a remote view and controls over your system to determine if there is any problem.



Chapter 12. Remote Web Client and SPhone Client for Simple Use

(Optional)

For remote users, there are 3 methods for viewing.

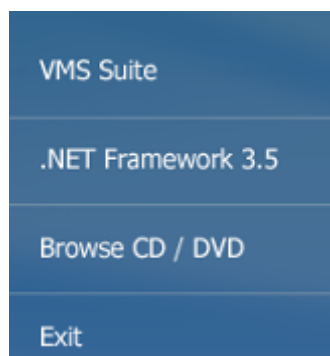
1. Remote Client: install Remote Client on remote PCs for live view and playback.
2. Web Client: use the browser IE (Internet Explorer) and input the IP address of the camera for live view and playback.
3. Mobile Client: install the **Sphone Client** app on iOS or Android mobile devices for basic live viewing.

12.1. Software Installation for Remote Control

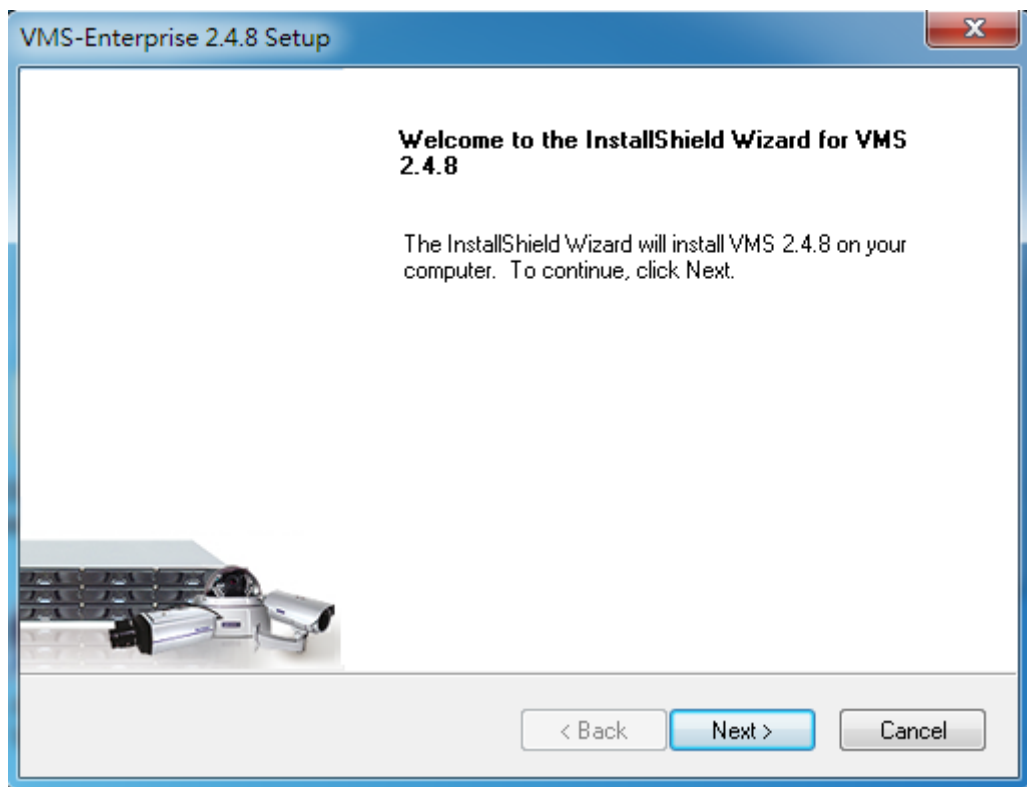
12.1. Installing the VMS

Note: For THE SYSTEM series, users have to install VMS Client on remote PC(s) when distant live viewing and playback are needed.

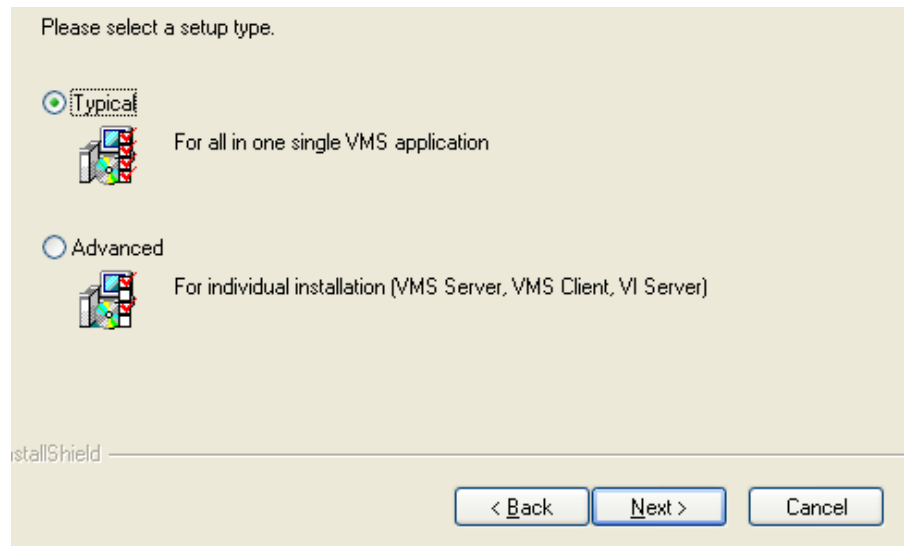
1. Insert the VMS/IPCAM CD-ROM. The CD should auto run. If it does not, open the CD manually and double-click **autorun.exe**. The menu below will be displayed.



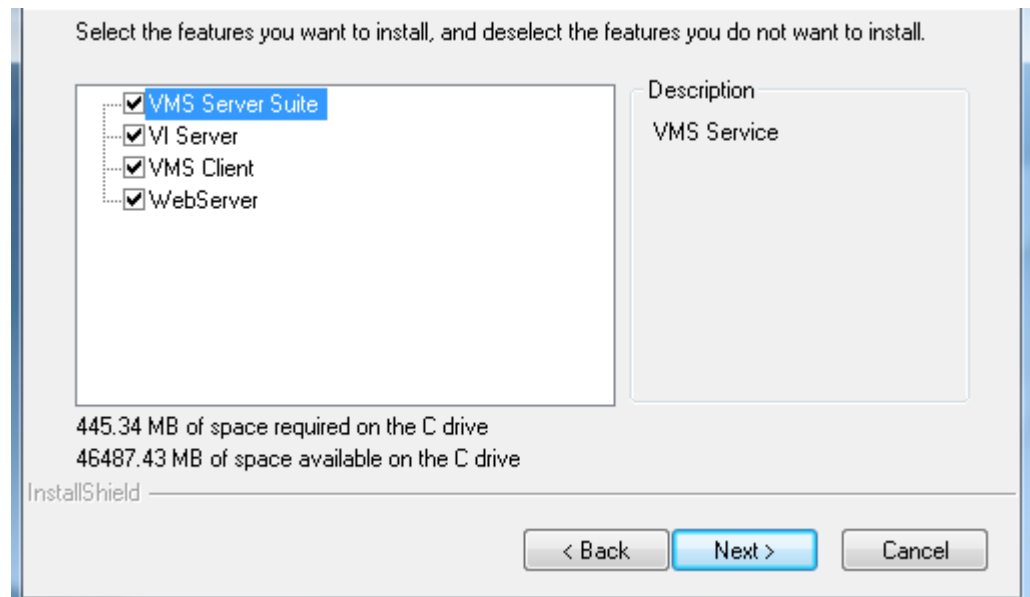
Click **VMS Suite** to start the installation.



2. Choose a setup type from *Typical* and *Advanced*. Then Click **Next** when you are satisfied with your selection.

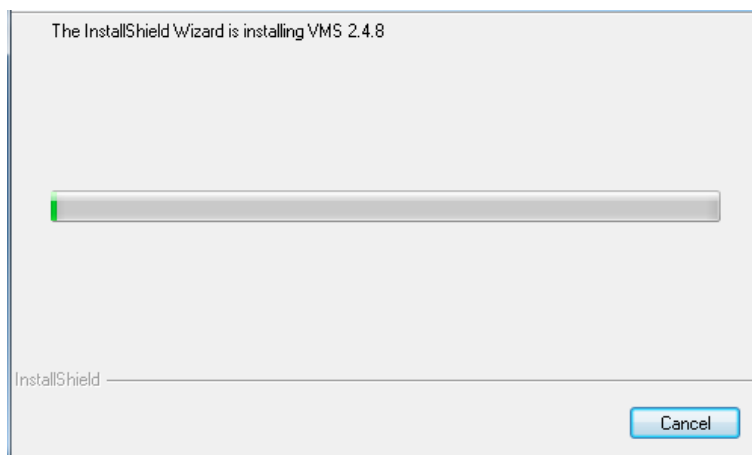
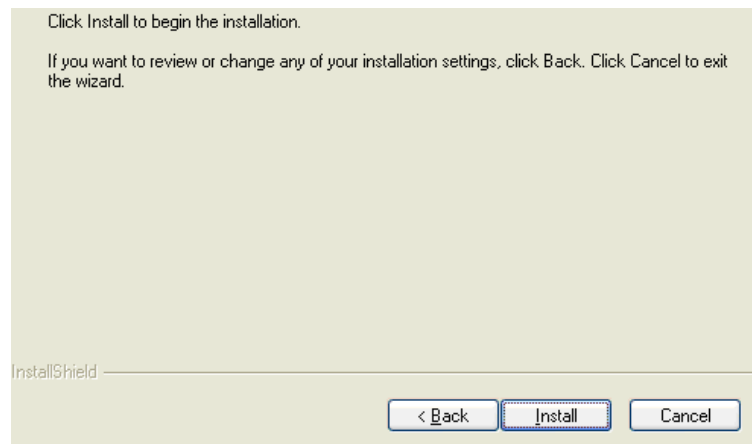


3. You may choose to install among the following while *Advanced Setup Type* is selected:

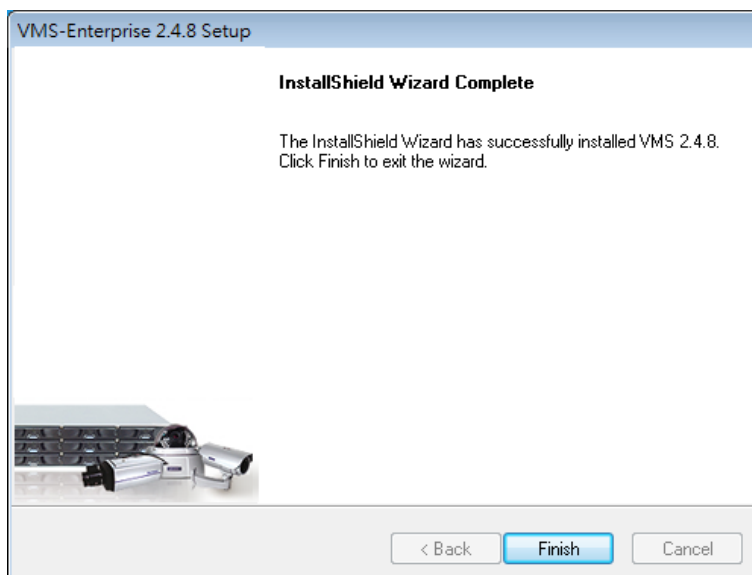


- **VMS Server Suite** - Includes the VMS Server and Local Domain Server, VI Server and VMS Client.
- **VI Server**
- **VMS Client**
- **Web Server**

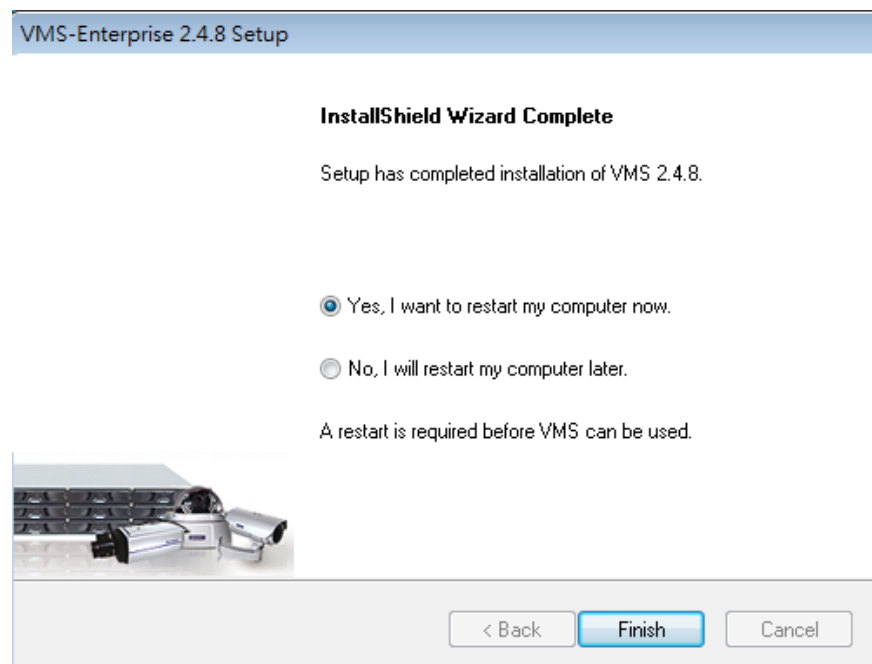
4. The confirmation screen will display. Click **Install**. A progress bar will display, indicating installation progress.



5. When installation is finished, an informational screen will display. Click **Finish** to complete installation.



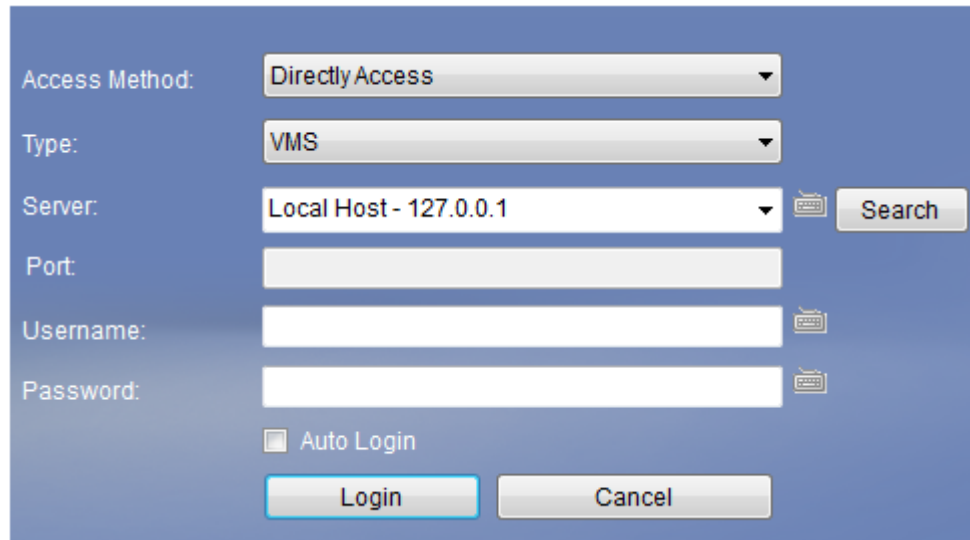
6. The system will prompt for a restart. A restart is required before the VMS will function correctly. You may choose to immediately automatically restart your computer, or restart your computer later. Clicking **Finish** will apply your choice.



12.2. Starting the VMS Client

To start the software, click **Programs > VMS Suite > VMS Client** under the Windows **Start** menu.

The software will prompt for the following information:



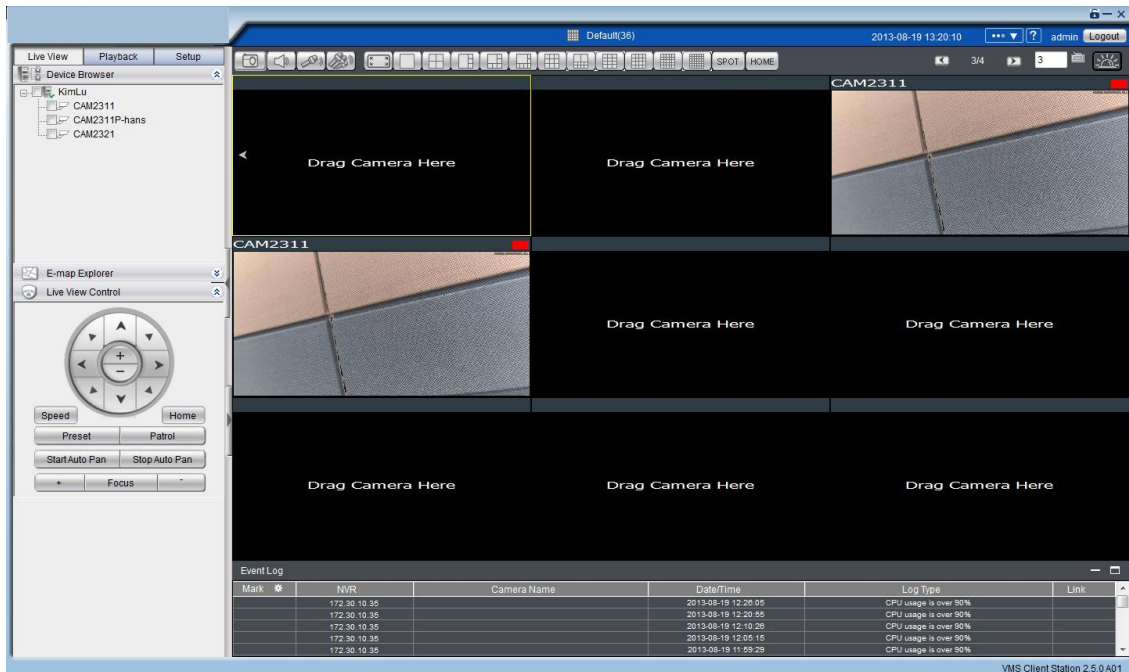
- **Access Method** - Directly Access or Internet Port Forward.
- **Type** - Choose VMS.
- **Server** - The IP address for the VMS/SMR Server. You can click **Search** button to obtain it. For users of port forwarding, it should be the IP address of the router.
- **Port** - The Login Port for port forwarding - 9050. It should be set under **Server > Other Tasks > Port Mapping** after the first login.

Note: (1) Please refer to *Port Forwarding Section* for more details. (2) SCC does not support port forwarding functionalities.

- **Username** - The username for the domain, **which is always *admin***.
- **Password** - The password for the domain. **Default password is *admin***.

Click **Login** after the password (and port number) is entered.

After logged in, you'll see the following images.



For VMS Remote Client configurations, please refer to the VMS User Manual.

12.2.1. Logging out

The Client can be logged out of all the Servers configured on the system by pressing the **Logout** button on the upper right hand corner in the GUI. Logging out of individual servers can be achieved by double clicking the server entry and clicking the **Yes** button on the confirmation screen.

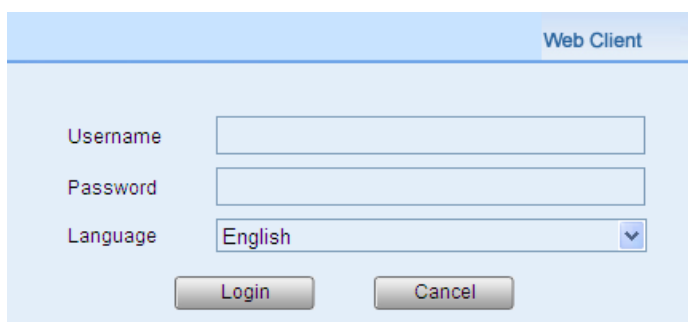
Note: (1) If the system becomes unresponsive, users can force shutdown the system (press and hold the power until the system shuts down). This should only be done when the system is unresponsive!

12.3. Starting the Web Client

Launch Microsoft Internet Explorer 7.0 (or above) and enter your **VMS Server IP address + “/webclient”** in your web browser’s URL location, e.g. <http://172.18.6.9/webclient> to download the Web Client application.

Note: Please check the web server settings in the VMS Setup first.

After the Web Client installation is done, a login window will pop up.

A screenshot of the Web Client login window. The window has a light blue header with the text "Web Client". Below the header, there are three input fields: "Username", "Password", and "Language". The "Language" field is a dropdown menu currently showing "English". Below the input fields are two buttons: "Login" and "Cancel".

- **Username** - The username for the domain. Default username is *admin*.
- **Password** - The password for the domain. Default password is *admin*.
- **Language** - Options for the interface languages.

Click **Login** after the username and password are entered.

After logging in, the live view page will be displayed on the web browser.

12.3.1. Checking the Software Version

Users can see the software version at the lower left corner of the window after logging in.

12.3.2. Use of 1x/4x views

Users have the option of viewing up to 4 recorded video streams at once, or just one stream at a time. Either of these options can be chosen by clicking on corresponding button in the button area above the main view screen. In both cases functionality and operation is the same.



12.3.3. PTZ Control

Cameras equipped with Pan-Tilt-Zoom functionality can be controlled directly within the Web Client. These controls can be found in the *PTZ Control* window within the live view screen.



12.3.4. Playback Settings



Users can select the (1) time and (2) camera, and then use the (3) time line and playback control panel to do the playback.

Note: For more details of PTZ Control and Playback Control, please refer to PTZ Control and Playback sections in this chapter.

12.4. Installing and Starting the SPhone Client on iOS Devices

12.4.1. Installing the SPhone Client (Optional)

Download the SPhone Client from App Store on the iPhone desktop.

12.4.2. Starting the SPhone Client

Note: Please check the web server settings in the VMS Setup first.

After the SPhone Client installation is done, a login window will pop up.

SPhone Client [Connect](#)

Connection Settings

Address
192.168.2.149

Port
80

Username
admin

Password
.....

☒ Remember me

3.0.0

- **Address:** The IP address for the VMS/SMR Server.
- **Port:** The login port for SPhone Client. **Default port number is 80.**

Note: The port number should be the same with the web server port.

- **Username** - The username for the domain. **Default username is *admin*.**
- **Password** - The password for the domain. **Default password is *admin*.**

Click **Connect** on the upper right corner after the port, username and password are entered.

12.4.3. Checking the Software Version

Users can see the software version at the lower right corner of the window after logging in.

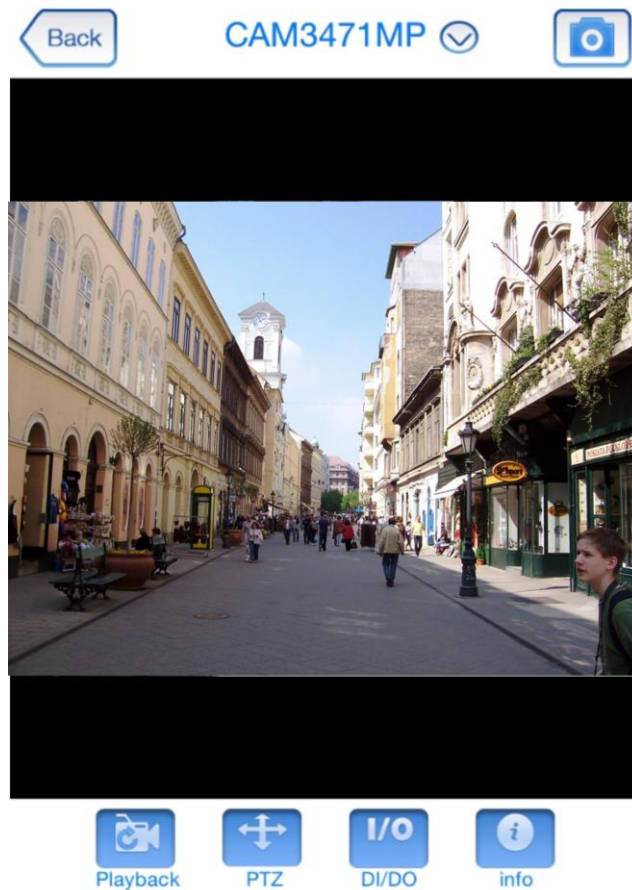
12.4.4. Functionalities on the SPhone Client

Live View









After logging in, you will see the Live View images. The default is 6 channels per page.



You can click on any channel you'd like to see or manage to have a single view on your device.



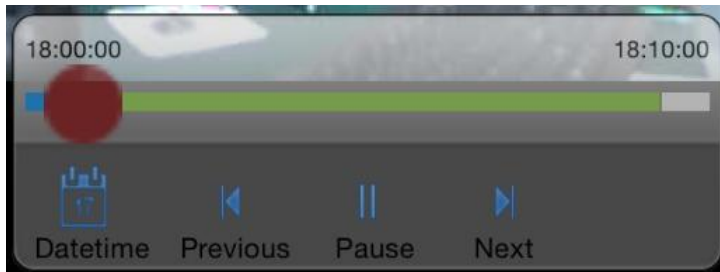
Icon Descriptions

Icon	Function
	Use the Back icon to go back to the previous page.
	Use the snapshot icon to take a snapshot of the current view.
	After tapping this icon, there'll be a drop-down list for you to select a camera to view or manage.
	Use the playback icon to view the recorded video from the current camera.
	Use the PTZ icon to perform a Pan, tilt, zoom functionality.
	<p>After tapping the PTZ icon, you'll also see a Preset icon. Use the Preset icon to monitor the set preset points.</p> <p>Presets should be made beforehand. Refer to the Chapter 8 for PTZ Preset settings.</p>
	Tap the icon to see the camera digital input/output status.
	Tap the icon to see a detailed information

Playback

After tapping on the Playback icon ,  you'll see the image below.

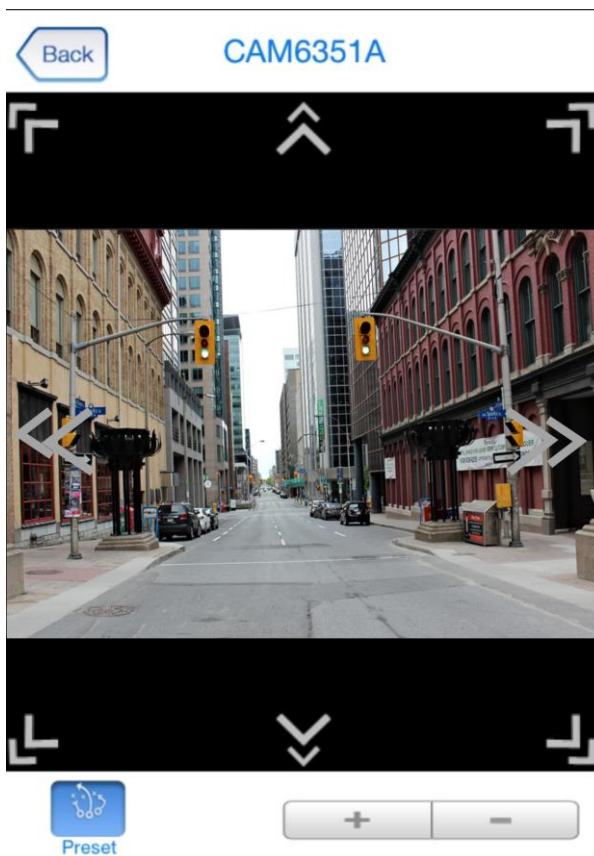
Use the icons on this page to set the date/time to search for the specified videos and use the Previous/Next, Play/Pause icons to view the recorded videos.



PTZ/Preset

After tapping the PTZ icon, you'll also see a Preset icon. Use the Preset icon to monitor the set preset points.

Presets should be made beforehand. Refer to the Chapter 8 for PTZ Preset settings.




DI/DO

Tap this icon to see the camera digital input/output status.

<div>Back</div> <div>CAM3471MP</div>	
Name	Status
Data Input1	<div></div>
Data Input 2	<div></div>
Data Output1	<div></div>

Info

The  icon can be used to check the detailed information of each camera as follows.

<div>Back</div> <div>CAM3471MP</div>	
Item	Specification
NVR Server	SMR8300
IP Address	192.168.2.120
Resolution	2048x1536
Quality	Medium
Frame rate	8

- **NVR Server:** The VMS/SMR Server name
- **IP Address:** The IP address for the VMS/SMR Server
- **Resolution:** The video resolution of the camera
- **Quality:** The video quality of the camera
- **Frame Rate :** The frame rate of the camera

12.5. Installing and Starting the SPhone Client on Android Devices

12.5.1. Installing the SPhone Client (Optional)

Download the SPhone Client from App Store on the Android phone desktop.

12.5.2. Starting the SPhone Client

Note: Please check the web server settings in the VMS Setup first.

After the SPhone Client installation is done, a login window will pop up.

- **Server Name:** The VMS/SMR Server Name
- **Address:** The IP address for the VMS/SMR Server.
- **Port:** The login port for SPhone Client. **Default port number is 80.**

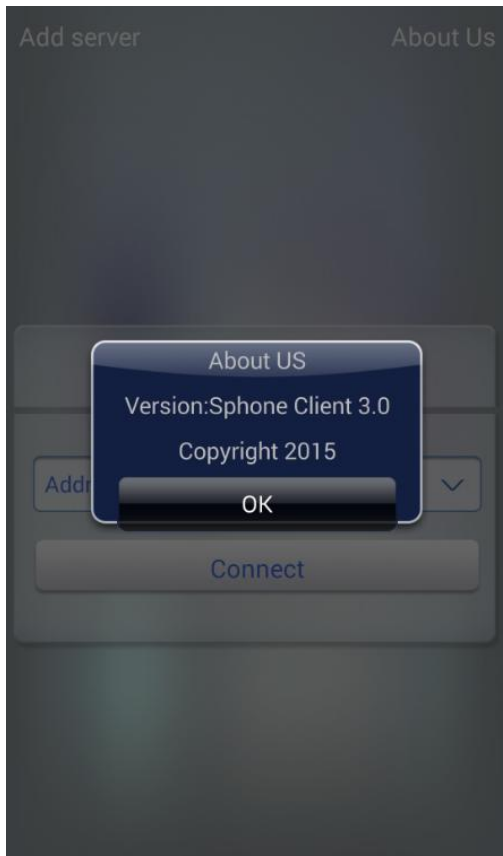
Note: The port number should be the same with the web server port.

- **Username** - The username for the domain. **Default username is *admin*.**
- **Password** - The password for the domain. **Default password is *admin*.**

Click **OK** icon after the port, username and password are entered.

12.5.3. Checking the Software Version

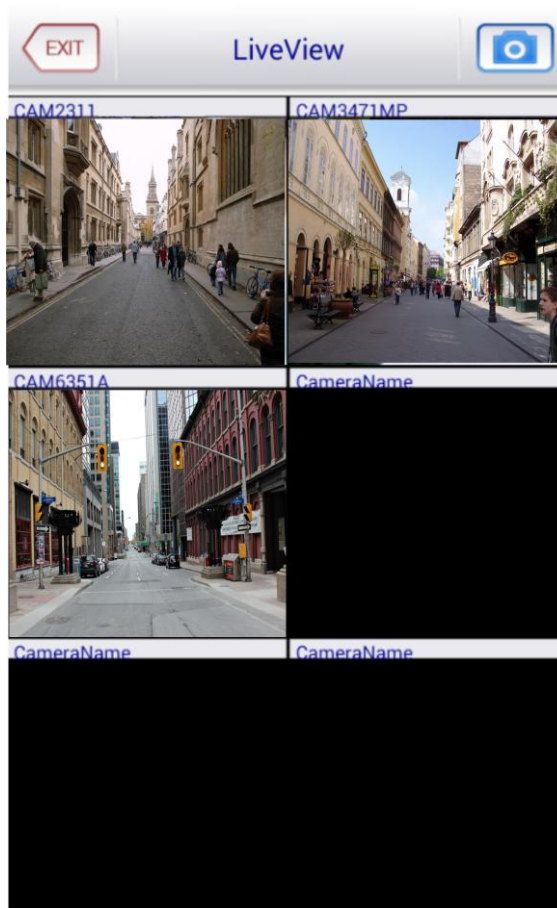
Users can see the software version. Tap on the About Us on the upper right corner of the window after logging in.



12.5.4. Functionalities on the SPhone Client

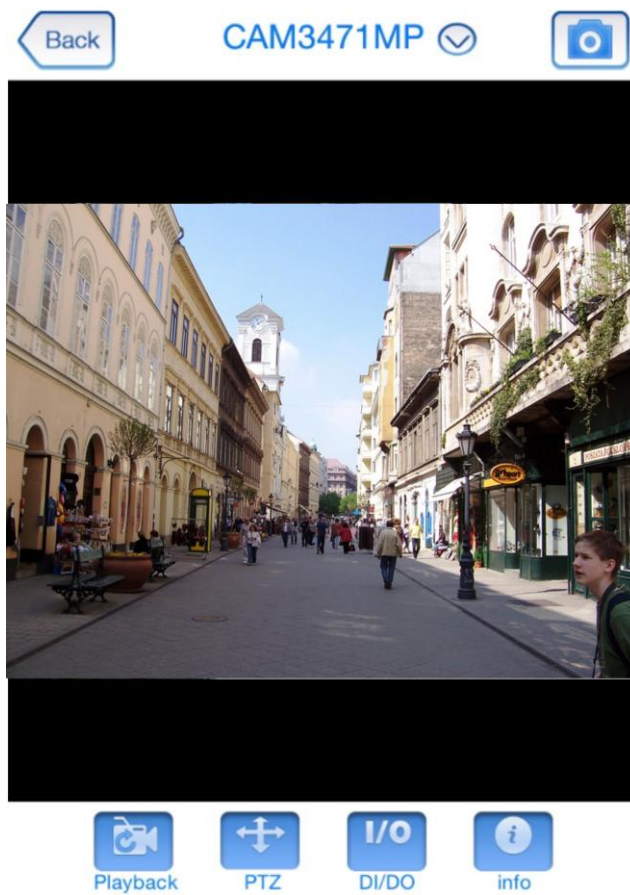
Live View

After logging in, you will see the Live View images. The default is 6 channels per page.











At most 6-channel live view can be displayed in the same page.

You can click on any channel you'd like to see or manage to have a single view on your device.



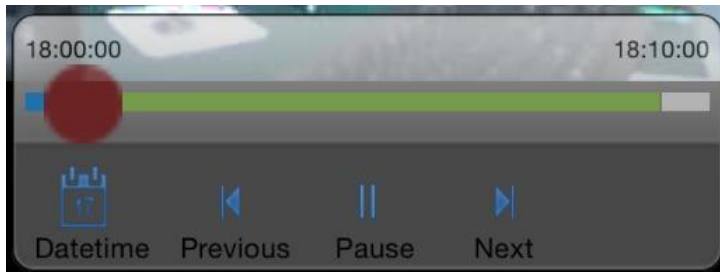
Icon Descriptions

Icon	Function
	Use the Back icon to leave this page.
	Use the snapshot icon to take a snapshot of the current view.
	After tapping this icon, there'll be a drop-down list for you to select a camera to view or manage.
	Use the playback icon to view the recorded video from the current camera.
	Use the PTZ icon to perform a Pan, tilt, zoom functionality.
	<p>After tapping the PTZ icon, you'll also see a Preset icon. Use the Preset icon to monitor the set preset points.</p> <p>Presets should be made beforehand. Refer to the Chapter 8 for PTZ Preset settings.</p>
	Tap the icon to see the camera digital input/output status.
	Tap the icon to see a detailed information

Playback

After tapping on the Playback icon ,  you'll see the image below.

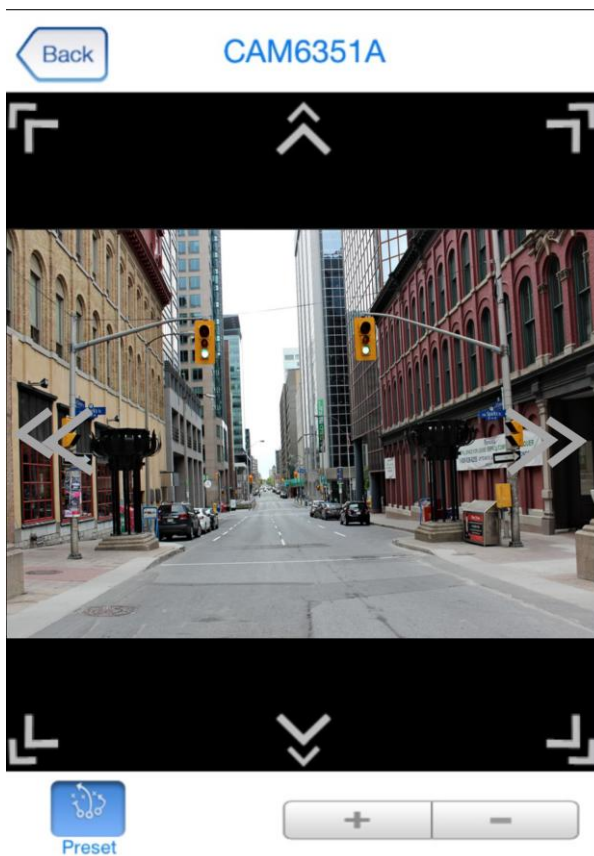
Use the icons on this page to set the date/time to search for the specified videos and use the Previous/Next, Play/Pause icons to view the recorded videos.



PTZ/Preset

After tapping the PTZ icon, you'll also see a Preset icon. Use the Preset icon to monitor the set preset points.

Presets should be made beforehand. Refer to the Chapter 8 for PTZ Preset settings.



DI/DO

Tap this icon to see the camera digital input/output status.




CAM3471MP



Name	Status
Data Input1	●
Data Input 2	●
Data Output1	●

Info

The icon  can be used to check the detailed information of each camera as follows.



CAM3471MP

Item	Specification
NVR Server	SMR8300
IP Address	192.168.2.120
Resolution	2048x1536
Quality	Medium
Frame rate	8

- **NVR Server:** The VMS/SMR Server name
- **IP Address:** The IP address for the VMS/SMR Server
- **Resolution:** The video resolution of the camera
- **Quality:** The video quality of the camera
- **Frame Rate :** The frame rate of the camera

Chapter 13. SurveOne (Optional)

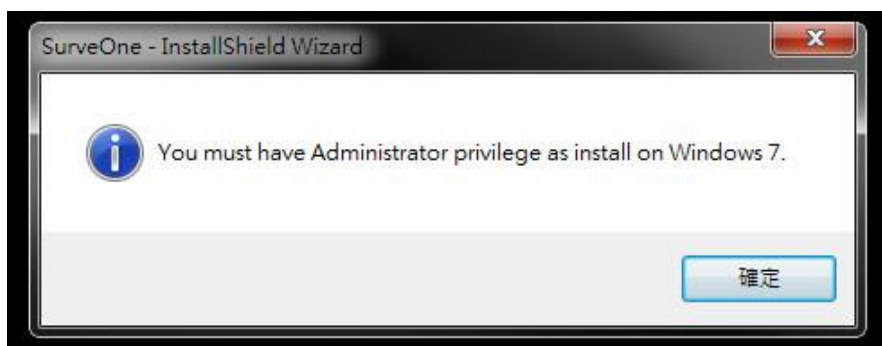
SurveOne is a smart web-based system health check tool. The health of the overall systems, including NVRs, cameras, and storage is constantly monitored to achieve the system stability. SurveOne can also simplify setup allowing users to copy the hardware configurations and apply them to other devices to save time and efforts. For easy maintenance, the 3 level-classified real-time event logs, critical errors, errors and warnings, help users to take action efficiently, and thus mitigate risks and reduce losses.

13.1. Installation

Once you have the software file, click to install and follow the installation steps.

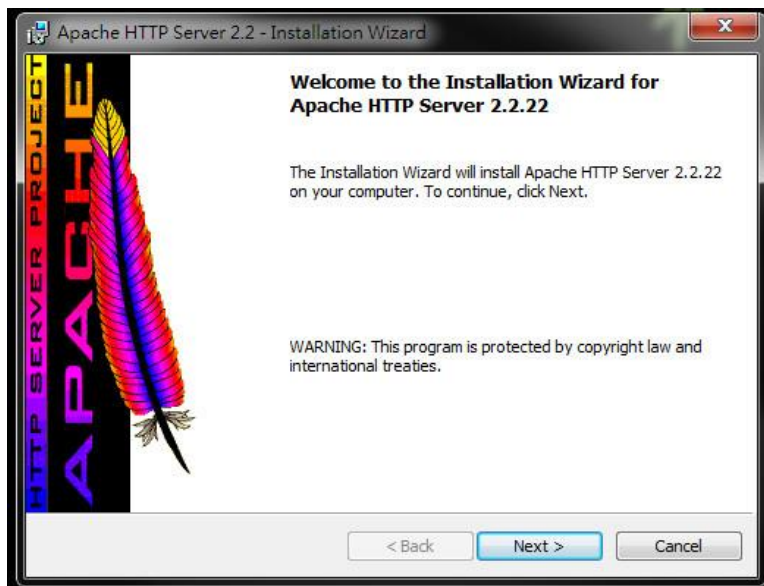


The system will warn you that you'll need to have the administrator privilege as install on Window 7.

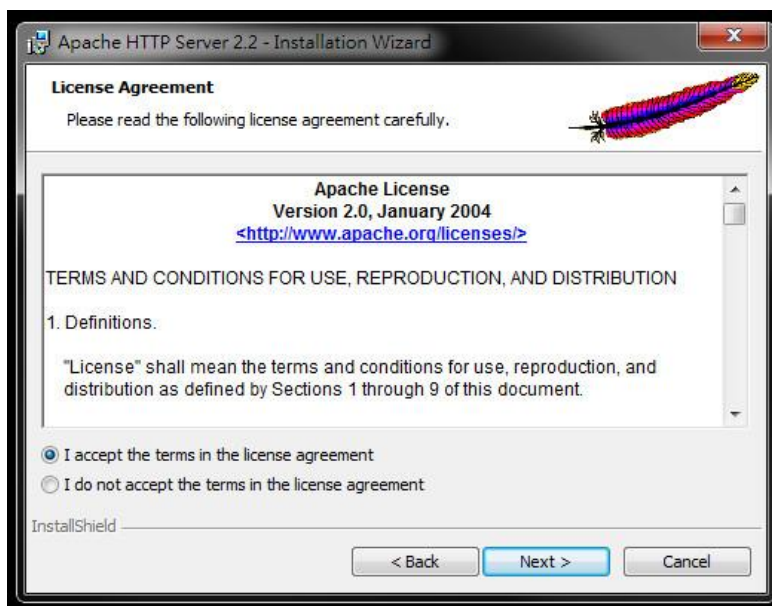


After confirmation, you can start the installation.

1. The installation wizard started. Click **Next**.



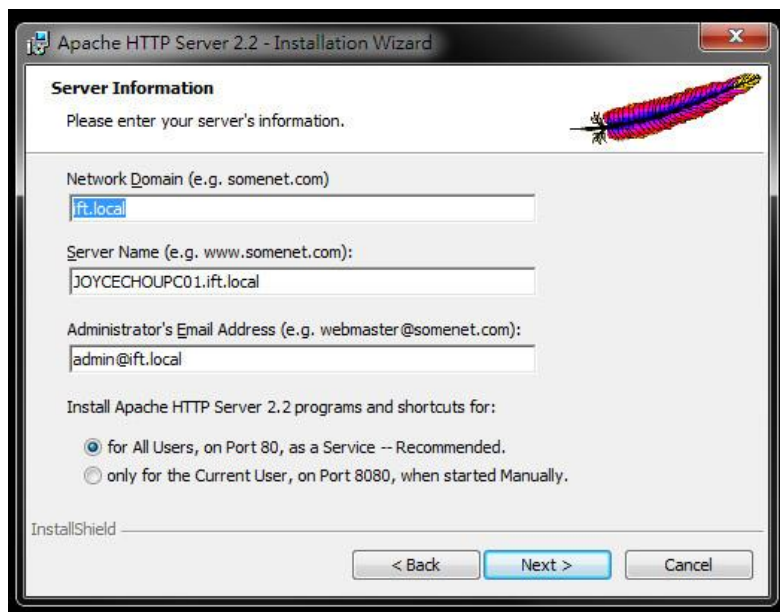
2. Accept the terms in the license agreement and click **Next**.



3. Accept and click **Next**.

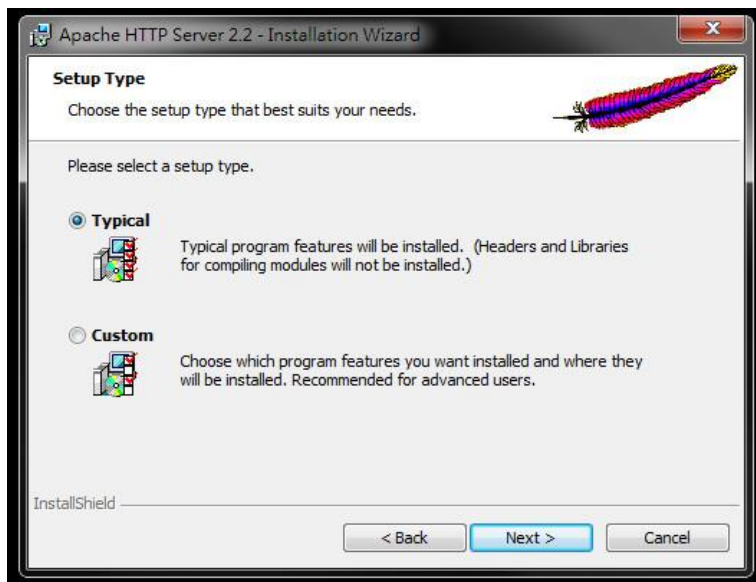


4. See if there's any information you'd like to change, if not click **Next**.

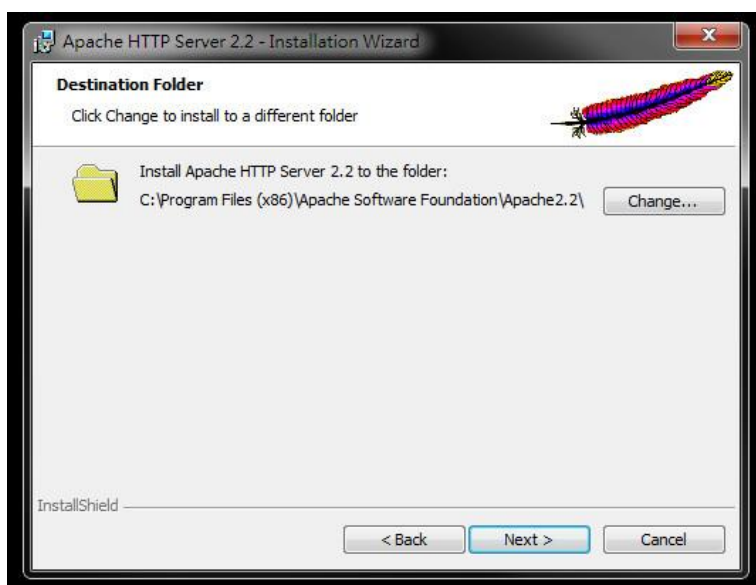


5. Select the setup type, typical or custom and click **Next**.

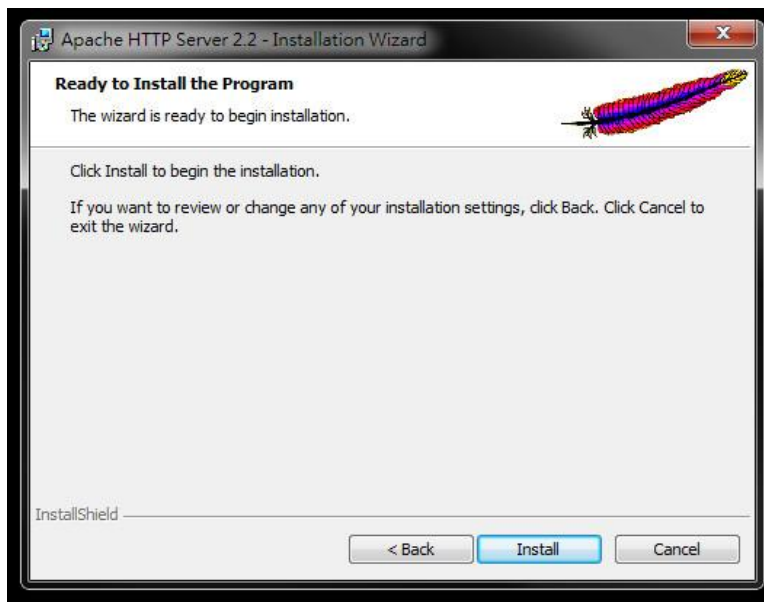
If you are not sure which one to select, it is recommended to select Typical.



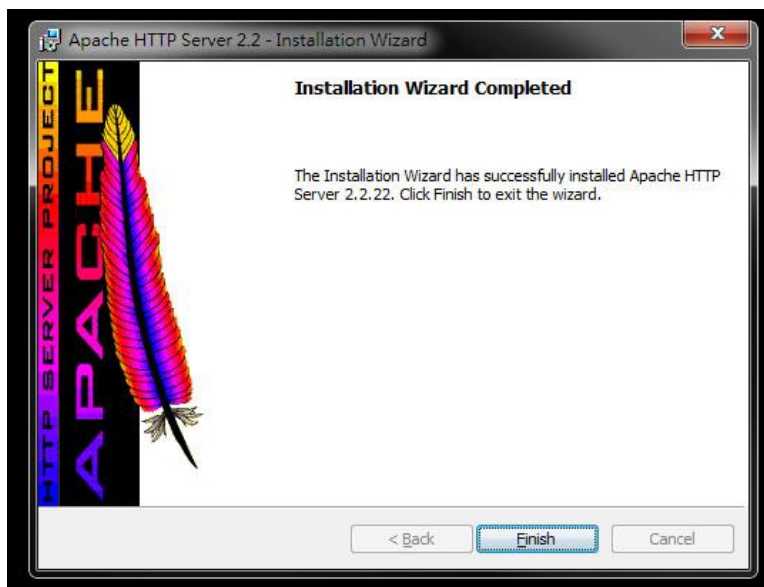
6. See if you'd like to change the destination folder, click **Change**, if not click **Next**.



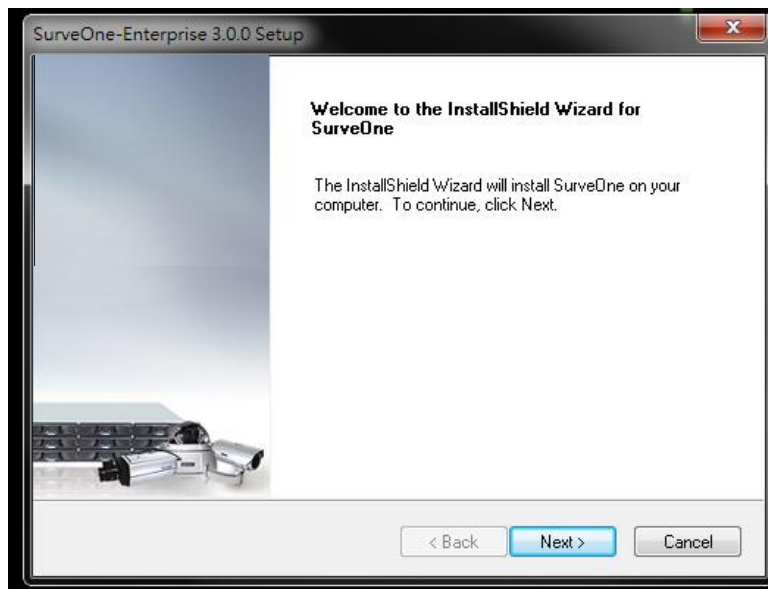
7. Click **Install** to start the installation.



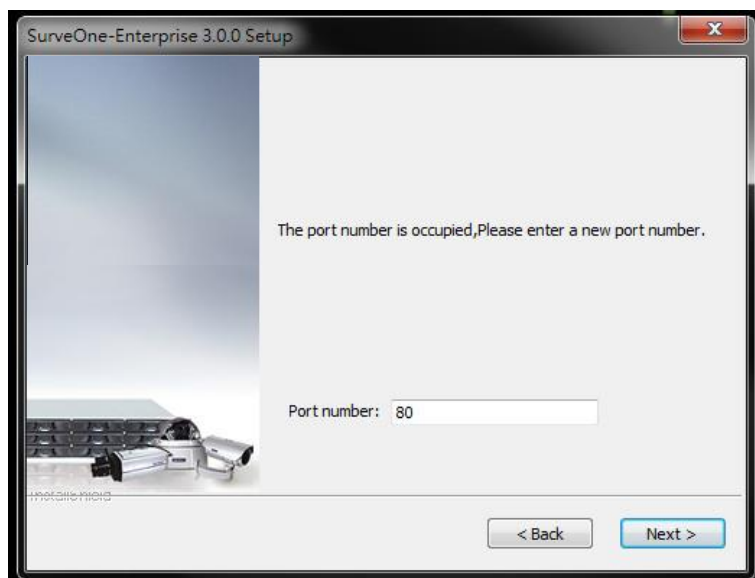
8. When the installation wizard completed, click **Finish**.



9. Then the SurveOne Installation Wizard will start. Click **Next**.

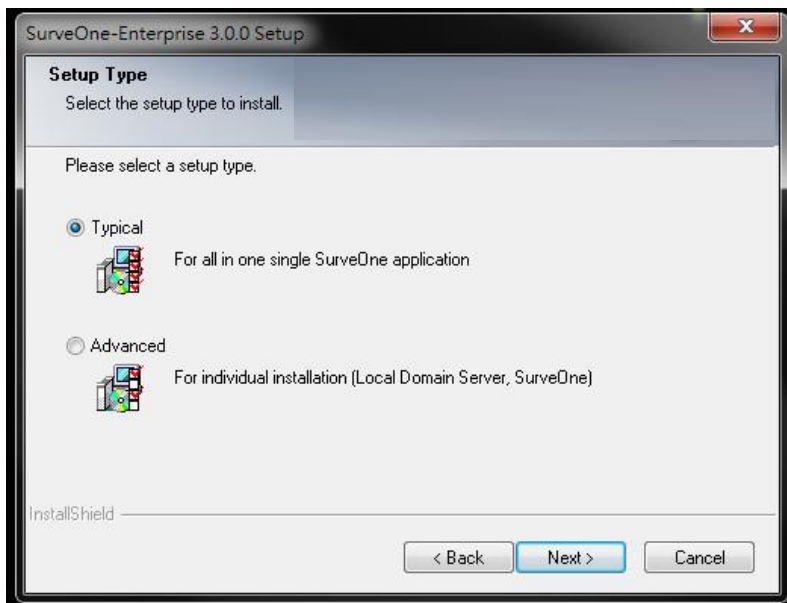


10. Input the port which is not occupied and click **Next**.

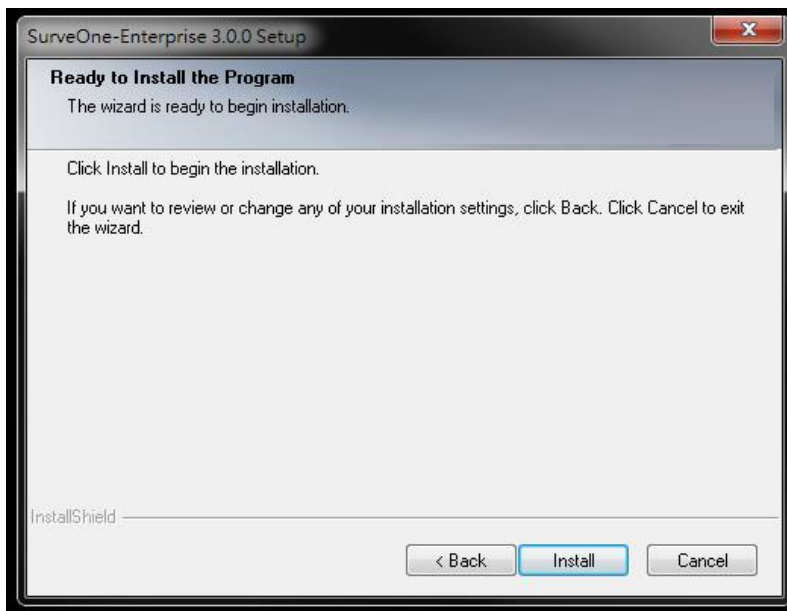


11. Select the setup type, Typical or Advanced and then click **Next**.

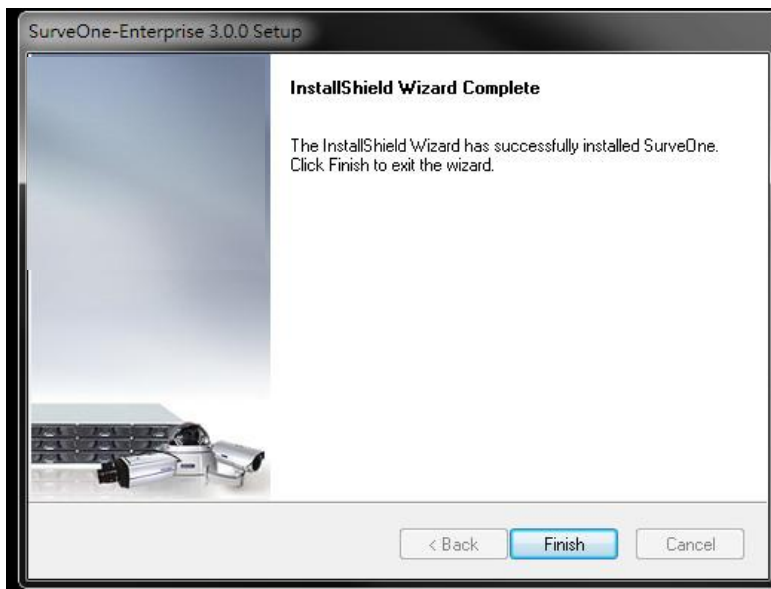
If you are not sure which one to select, it is recommended to select Typical.



12. Start to install the SurveOne.



13. Once the installation is complete, click **Finish**.



14. Restart your computer to activate the changes. Click **Finish** to exit.



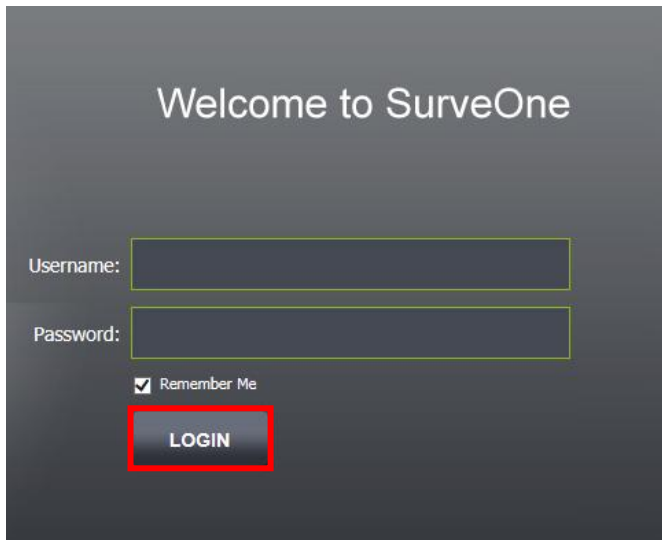
15. After the installation is done and your computer is restarted. On your desktop you'll find an IE browser icon with SurveOne on it. Double click this icon to log in to the SurveOne and start monitor the overall system status.



13.2. Login

Log in to SurveOne:

1. Go to <http://127.0.0.1:XX> (XX is the port you have setup in the installation wizard.)
2. Input the default username and password, admin and admin.
3. Click **LOGIN**.

The image shows the SurveOne login interface. At the top, it says "Welcome to SurveOne". Below this, there are two input fields: "Username:" and "Password:". The "Remember Me" checkbox is checked. A red rectangle highlights the "LOGIN" button.

Welcome to SurveOne

Username:

Password:

☒ Remember Me

LOGIN

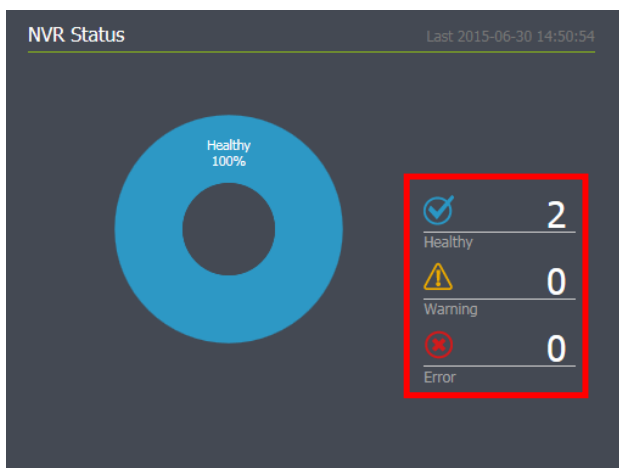
13.3. Overview

Real-time System Status Information - The overall status of NVRs, cameras, and storage is displayed graphically, allowing users to grasp how the systems are at a glance.



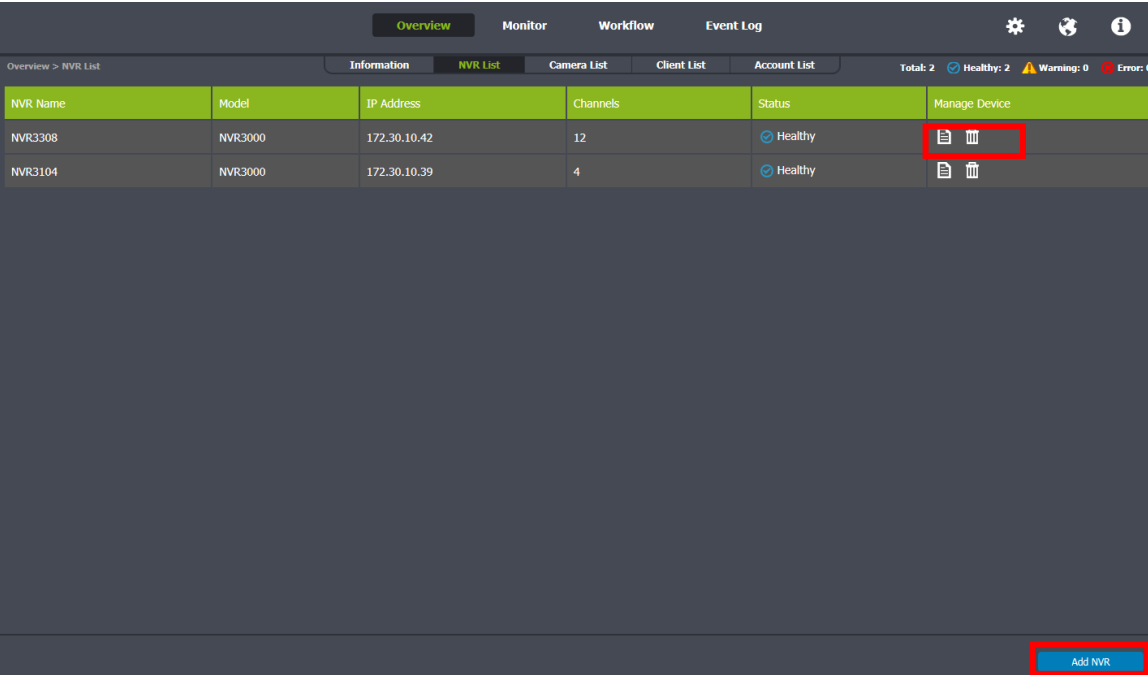
13.3.1. NVR Status


NVR status is classified into 3 groupings, Healthy, Warning and Error. Click on the status to see the details.

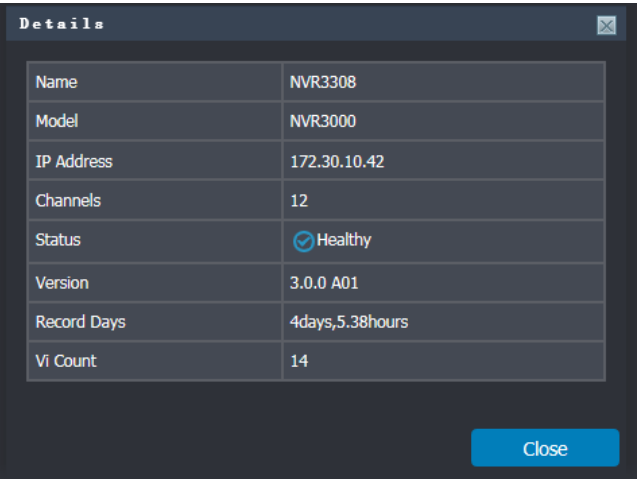


13.3.2. NVR List

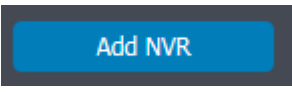
After clicking on the status, the system will take you to the NVR List to see the detailed NVR status with information such as NVR name, model, IP address, channels and status.

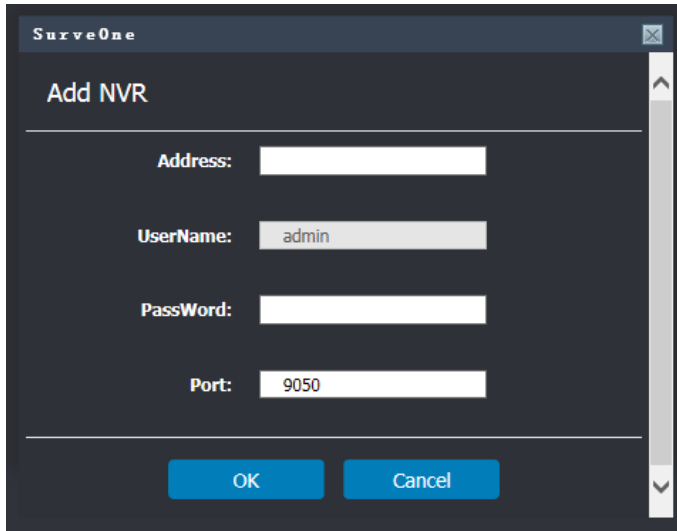


Click on the  to see the details of the NVR, including name, model, IP address, channels, status, version, record days, and VI counts.



Click on the  to remove the NVR.

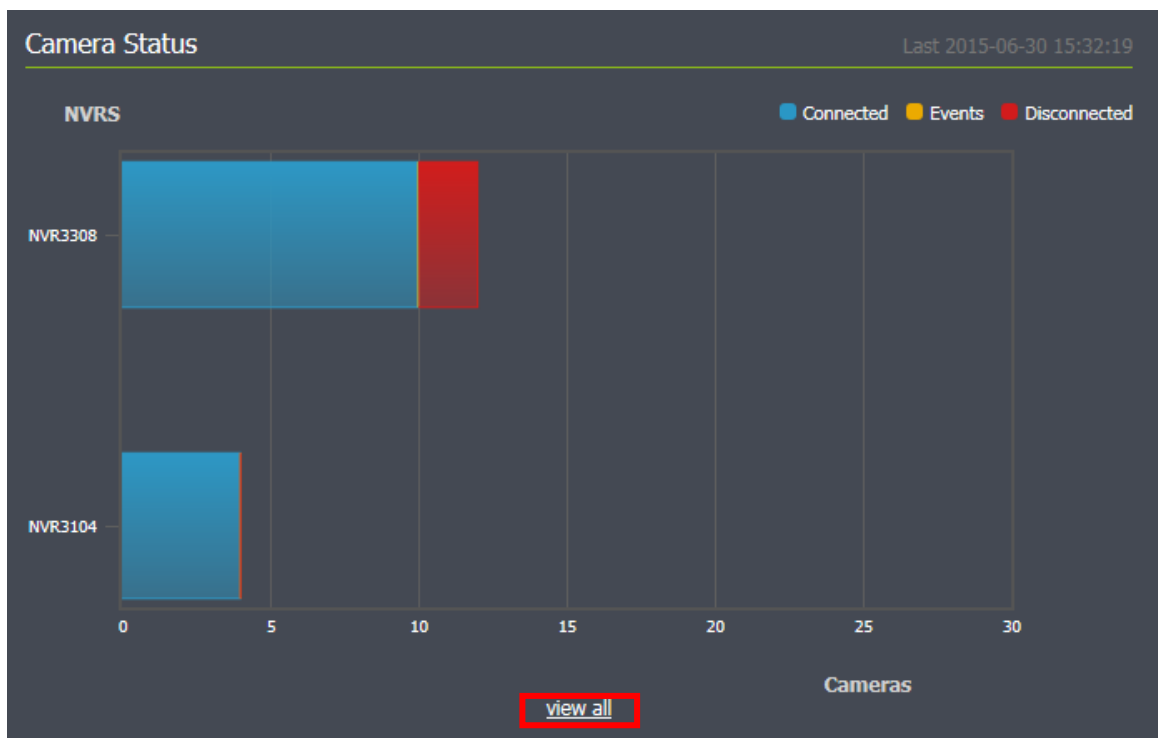
Click  and fill out the pop-up form to add NVR.



The image shows a 'SurveOne' window titled 'Add NVR'. It contains four input fields: 'Address:' (empty), 'UserName:' (containing 'admin'), 'PassWord:' (empty), and 'Port:' (containing '9050'). At the bottom are 'OK' and 'Cancel' buttons.

13.3.3. Camera Status

Camera status is classified into 3 groupings, Connected, Events, and Disconnected. Click on the [view all](#) to see the details.



13.3.4. Camera List


After clicking on the view all, the system will take you to the Camera List to see the detailed Camera status with information such as camera name, model, IP address, and status. Cameras under different NVR will be listed separately.


Overview				
Overview > Camera List				
Information NVR List Camera List Client List Account List				
Total:13 Connected:10 Events:1 Disconnected:2				
NVR	Camera Name	Model	IP Address	Status
NVR3308 (172.30.10.42)	IPCAM	CAM1200	172.30.10.70	Connected
NVR3104 (172.30.10.39)	CAM6181	CAM6181	172.30.10.181	Connected
	CAM6351	CAM6351	172.30.10.250	Event
	CAM2311	CAM2311	172.30.10.97	Connected
	CAM2331	CAM2331	172.30.10.104	Connected
	CAM1301	CAM1301	172.30.10.99	Disconnected
	CAM2311	CAM2311	172.30.10.70	Connected
	CAM2441	CAM2441	172.30.10.55	Connected
	CAM4361LV-2	CAM4361LV-2	172.30.10.93	Connected
	ONVIF	ONVIF	172.30.10.82	Connected
	ONVIF	ONVIF	172.30.10.61	Connected
	ONVIF	ONVIF	172.30.10.66	Connected
	ONVIF	ONVIF	172.30.10.95	Disconnected


13.3.5. Events Status

NVR and camera event logs are presented in real-time and classified into 3 groups: critical error, error, and warning, for easy management.

Events


Critical Error
0


Error
0


Warning
0

Since 2015-06-30 15:30:12

Latest Events

Critical Error
None

Error
2015-06-30 15:17:29 NVR3308: Video Loss Happened[5]

Warning
None

13.3.6. Event Log

After clicking on the Latest Events, the system will take you to the Event Log to see the detailed event status with information such as source, severity, date/Time and Event. With classified event logs, users can identify which event needs to take actions first and which not to respond to the situations more quickly and efficiently.

NVR	SOURCE	Severity	Date / Time	Event
NVR3308 (172.30.10.42)	IPCAM	✓	2015-06-30 14:44:27	admin 127.0.0.1 login success
NVR3104 (172.30.10.39)	NVR3308 (172.30.10.42)	✓	2015-06-30 14:46:08	NVR service start
	CAM1301	⚡	2015-06-30 14:46:18	Video Loss Happened[5]
	ONVIF	⚡	2015-06-30 14:46:18	Video Loss Happened[11]
	ONVIF	⚡	2015-06-30 14:46:19	Video Loss Happened[12]
	CAM2311	✓	2015-06-30 14:46:34	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:37	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:40	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:43	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:46	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:49	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:52	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:55	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:57	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:47:00	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:47:04	VI(camera motion) happened

Use the drop-down list to filter the specific event, such as All, Normal, Warning, Error, Critical Error, you'd like to search and click Search or Export.

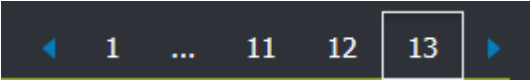
NVR	SOURCE	Severity	Date / Time	Event
NVR3308 (172.30.10.42)	CAM6351	✓	2015-06-30 15:41:48	VI(camera motion) happened
NVR3104 (172.30.10.39)	CAM6351	✓	2015-06-30 15:41:51	VI(camera motion) happened
	CAM6351	✓	2015-06-30 15:41:55	VI(camera motion) happened
	CAM6351	✓	2015-06-30 15:41:57	VI(camera motion) happened
	CAM6351	✓	2015-06-30 15:42:00	VI(camera motion) happened

Click Export, the log you're looking for will be copied to the notebook as shown below.

```

NVR3308_log_记录本
-----
日期时间  级别  类型  内容
2015-06-30 15:13:15  level: 1 type: 1 content: Video Loss Happened[5]
2015-06-30 15:13:15  level: 1 type: 1 content: Video Loss Happened[11]
2015-06-30 15:17:29  level: 1 type: 1 content: Video Loss Happened[5]
2015-06-30 15:17:29  level: 1 type: 1 content: Video Loss Happened[11]
2015-06-30 15:17:29  level: 1 type: 1 content: Video Loss Happened[12]
2015-06-30 16:02:06  level: 1 type: 1 content: Video Loss Happened[5]
2015-06-30 16:02:07  level: 1 type: 1 content: Video Loss Happened[11]
  
```

Click on the number on the upper right corner to jump to the corresponding page to see the log.



13.3.7. Client List

See the client information such as the client IP address and the client version here.

Overview			Monitor	Workflow	Event Log		
Overview > Client List			Information	NVR List	Camera List	Client List	Account List
NVR	Client IP Address		Client Version				
NVR3308 (172.30.10.42)			Unknown				
NVR3104 (172.30.10.39)							

13.3.8. Account List

See the account information such as the account list and the status here.

Overview			Monitor	Workflow	Event Log		
Overview > Account List			Information	NVR List	Camera List	Client List	Account List
NVR	Account List		Status				
NVR3308 (172.30.10.42)	admin		Enable				
NVR3104 (172.30.10.39)	poweruser		Enable				
	user		Enable				
	viewer		Enable				

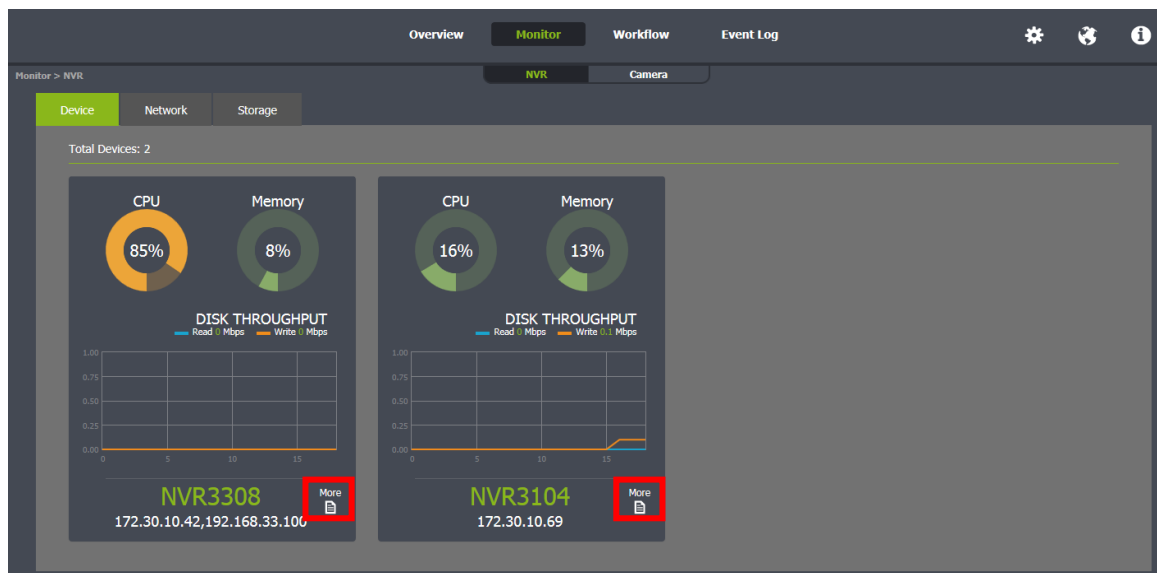
13.4. Monitor


As long as there is network connectivity, users can easily monitor the system status locally or remotely and ensure the consistent stability.

13.4.1. NVR

Device

See the connected NVR information including CPU, memory, and disk throughput graphically.



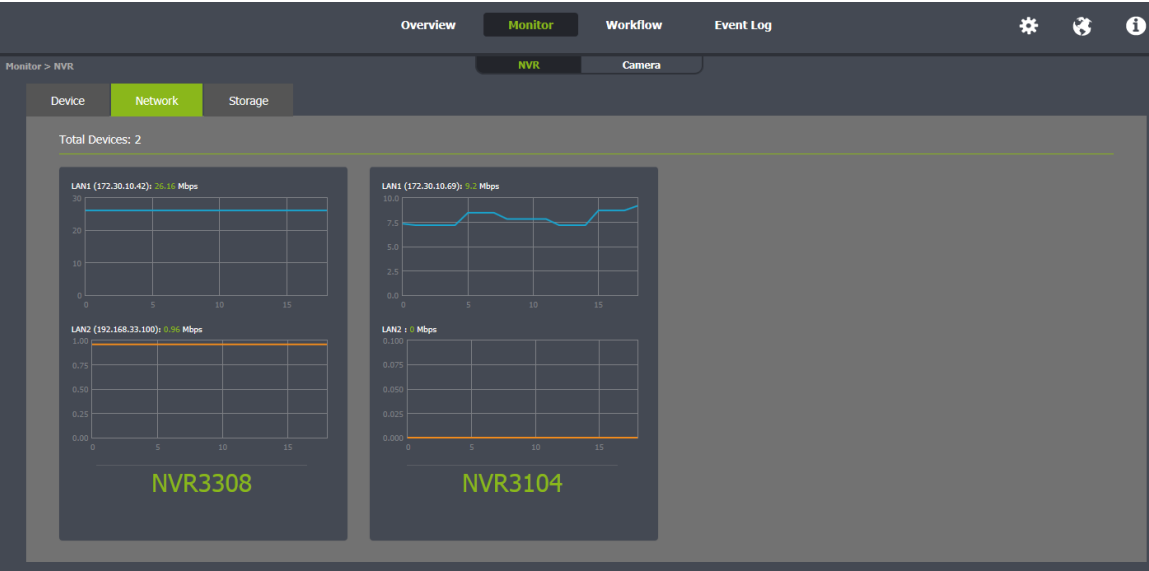
Click on the  to bring out the following chart to learn the details.

Details	
CPU	84.5%
Memory	7.9%
Disk Throughout	Read: 0 Mbps Write: 0 Mbps
Recording Days	4 days 6.74 hours
PSU0 Fan0	--
PSU0 Fan1	--
PSU1 Fan0	--
PSU1 Fan1	--

Close

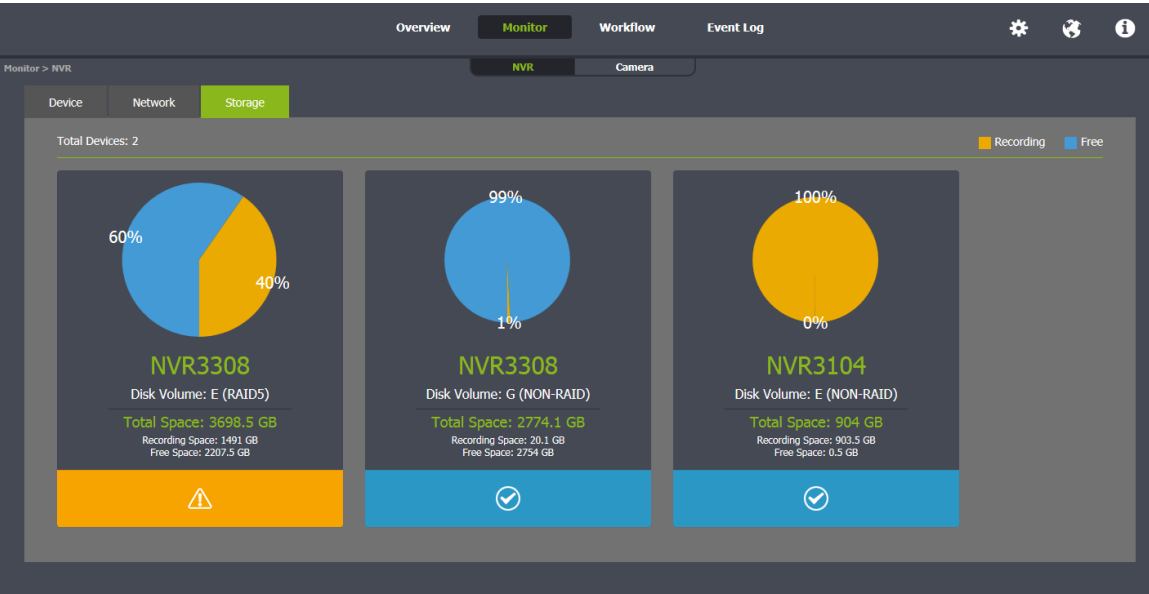
Network

See the network status graphically.






Storage

See the storage status including disk volume, space information graphically.




13.4.2. Camera

See the connected camera information including camera name, model, IP address, resolution, frame rate, bit rate, and status here.

Overview Monitor Workflow Event Log								
Monitor > Camera			NVR Camera		Total:13 Connected:12 Events:0 Disconnected:1			
NVR	Camera Name	Model	IP Address	Resolution	Frame Rate	Bit Rate	Status	View
NVR3308 (172.30.10.42)	IPCAM	CAM1200	172.30.10.70	1920x1080	15	979	Connected	
NVR3104 (172.30.10.39)	CAM6181	CAM6181	172.30.10.181	720x480	60	2157	Connected	
	CAM6351	CAM6351	172.30.10.250	1920x1080	30	3719	Connected	
	CAM2311	CAM2311	172.30.10.97	1920x1080	15	799	Connected	
	CAM2331	CAM2331	172.30.10.104	1280x1024	15	1036	Connected	
	CAM1301	CAM1301	172.30.10.99	0x0	0	0	Disconnected	
	CAM2311	CAM2311	172.30.10.70	1920x1080	15	979	Connected	
	CAM2441	CAM2441	172.30.10.55	1920x1080	15	1099	Connected	
	CAM4361LV-2	CAM4361LV-2	172.30.10.93	1920x1080	15	1257	Connected	
	ONVIF	ONVIF	172.30.10.82	2560x1920	30	4382	Connected	
	ONVIF	ONVIF	172.30.10.61	2560x1920	30	4384	Connected	
	ONVIF	ONVIF	172.30.10.66	1920x1080	30	2057	Connected	
	ONVIF	ONVIF	172.30.10.95	1920x1080	30	2299	Connected	

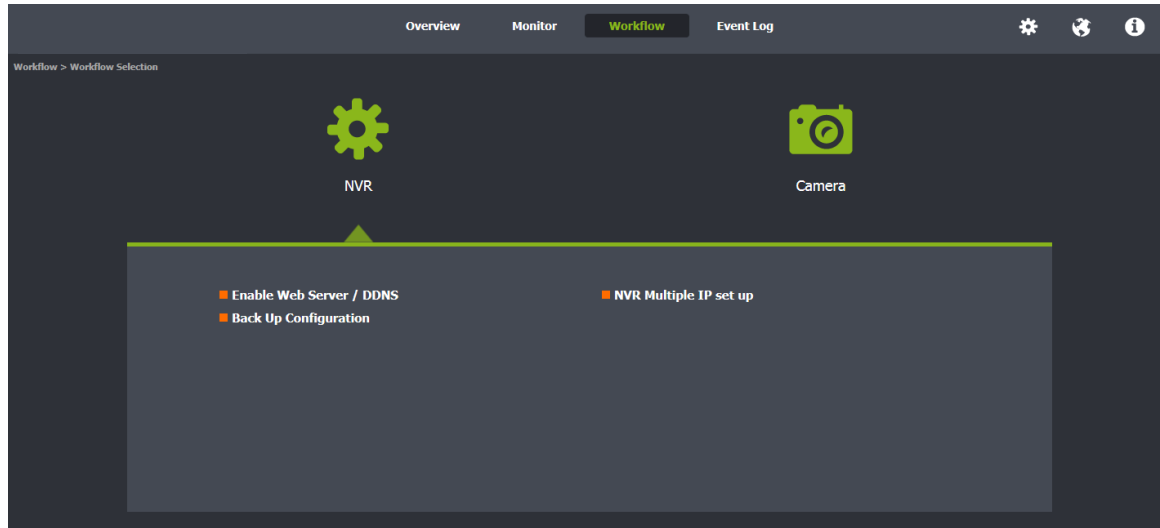


Click on the  to see more details, such as camera name, model, IP address, resolution, frame rate, bit rate, codec, and firmware version.

Details	
Camera Name	IPCAM
Model	CAM1200
IP Address	172.30.10.70
Resolution	Stream 1: 1920x1080 Stream 2: 320x240
Frame Rate	Stream 1: 15 Stream 2: 15
Bit Rate	Stream 1: 1050 Stream 2: 529
Codec	Stream 1: H264 Stream 2: H264
Firmware Version	V2.4.C10
Close	

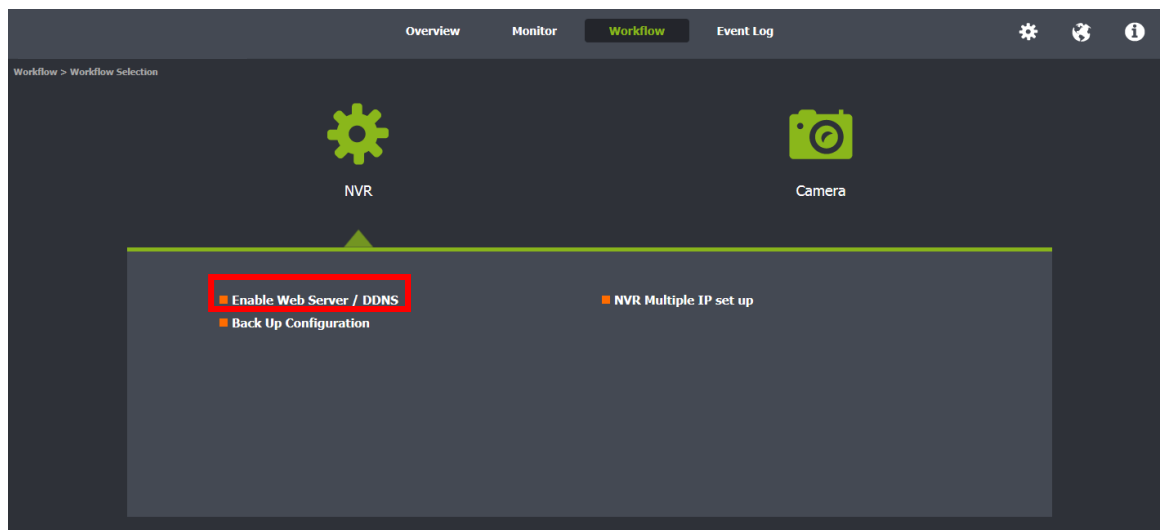
13.5. Workflow

Designed for easy configuration, deployment and maintenance, SurveOne allows users to do one-time setup. Users can simply copy the NVR or camera configurations and apply them to new devices to ease the complicated setup process. The configurations can also be saved as backup and restored when needed.



13.5.1. NVR

Enable Web Server / DDNS



Web Server

Follow the instruction flow on the right. Users can set up the Web server/DDNS here. Click **Enable** to activate the functionalities. You can also click **Advanced Setting** to fill in further information.

The screenshot shows the 'Configure Parameters' page for Web Server and DDNS configuration. The page has a dark theme with a top navigation bar containing 'Overview', 'Monitor', 'Workflow' (selected), and 'Event Log'. Below the navigation bar, the breadcrumb path is 'Workflow > NVR > Enable Web Server / DDNS'. The main content area is titled 'Configure Parameters'. On the left, there is a 'Select NVR' section with a dropdown menu showing 'NVR3308'. Below this, there are two sections: 'Web Server' and 'DDNS'. In the 'Web Server' section, the 'Enable' radio button is selected, and the 'Advanced setting' checkbox is checked. In the 'DDNS' section, the 'Enable' radio button is selected, and the 'Advanced setting' checkbox is checked. On the right side of the page, there is a vertical sidebar with three buttons: 'Web Server Configuration', 'DDNS Configuration', and 'Complete'. The 'Web Server Configuration' button is highlighted with a red box. At the bottom of the page, there are two buttons: 'Back to Workflow Selection' and 'Reset'.

Enable the Web Server and click **Advanced setting** to fill in the following information for the Web Server settings to use the Web Client/Mobile Client.

This screenshot shows the 'Configure Parameters' page with the 'Web Server' advanced settings expanded. The 'Web Server' section is highlighted with a red box. It contains the following fields: 'Web Server Port' (80), 'Web Stream Server Port' (8080), 'Max Connection' (40), 'FPS' (8), and 'Video Quality' (Medium). The 'DDNS' section is also visible, with the 'Advanced setting' checkbox checked. It contains the following fields: 'DDN Service' (dyndns), 'Host Name', 'User Name', and 'Password'. The right sidebar with 'Web Server Configuration', 'DDNS Configuration', and 'Complete' buttons is still visible. The bottom navigation bar includes 'Back to Workflow Selection', 'Reset', and 'Run' buttons.

Note: (1) User may just keep the default settings in the Web Server. (2) Do not set the Web Server Port as these port numbers - 8080 (Web Stream Port), 9090 (NVR Stream Port), 2809 (NVR Server Login Port), 7735 (TV Wall Port (2.5.0)), 7734, 1024, 9010 (Domain Broadcast Port), 9030 (Domain Client Message Port), 9040 (Domain Console Message Port), 9050 (Domain Local Communication Port), 9020 (Domain Remote Communication Port), 9080 (Domain Local Log Data Download Port), 9081 (Domain Remote Log Data Download Port), 9060 (Domain Local Data Port), 9061 (Domain Remote Data Port), 15507 (Domain Local Log Message Download Port), 15503 (Domain Remote Log Message Download Port), 15501 (Domain Remote Log Upload port), 15505 (Domain Local Log Upload Port), 40000 (NVR Broadcast Port), 50000 (NVR Message Port).

DDNS

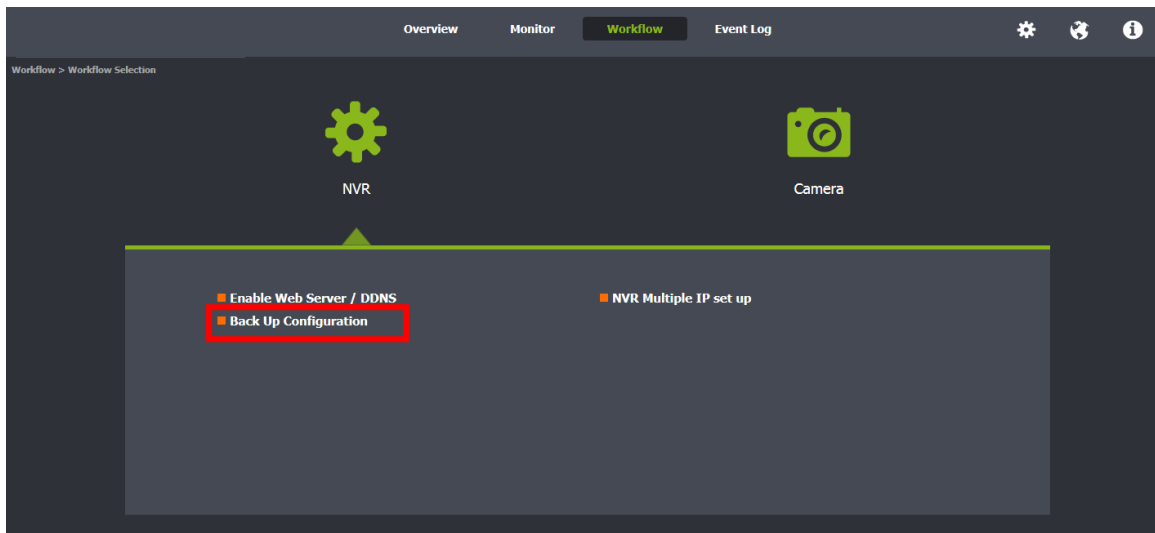
DDNS (Dynamic Domain Name Server) is a protocol that enables the device to maintain a static connection address, even when its IP changes. Access using this feature is disabled by default. Connecting using DDNS requires registration on third-party websites for DDNS services.

The screenshot shows the 'Configure Parameters' page for DDNS configuration. The interface includes a top navigation bar with 'Overview', 'Monitor', 'Workflow', and 'Event Log'. The main content area is titled 'Configure Parameters' and has a breadcrumb 'Workflow > NVR > Enable Web Server / DDNS'. On the right, there is a sidebar with 'Web Server Configuration', 'DDNS Configuration', and a 'Complete' button. The 'Web Server' section has radio buttons for 'Enable' and 'Disable', and a checked 'Advanced setting' checkbox. Below this are input fields for 'Web Server Port' (80), 'Web Stream Server Port' (8080), 'Max Connection' (40), 'FPS' (8), and 'Video Quality' (Medium). The 'DDNS' section, highlighted with a red box, also has 'Enable' and 'Disable' radio buttons, a checked 'Advanced setting' checkbox, and input fields for 'DDN Service' (dyndns), 'Host Name', 'User Name', and 'Password'. At the bottom, there are three buttons: 'Back to Workflow Selection' (highlighted with a red box), 'Reset', and 'Run' (both highlighted with red boxes).

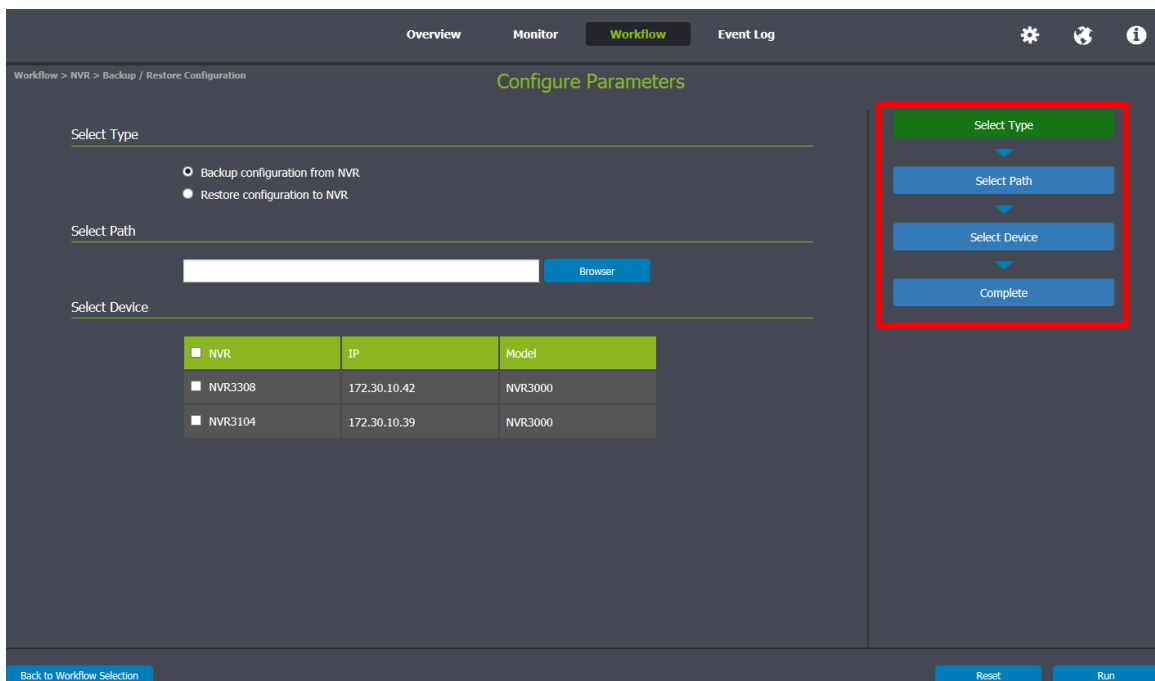
Check the **Enable DDNS** option and click **Advanced setting** to fill in valid user name and password. You can then access the device through the registered domain name.

- Click **Back to Workflow Selection** to go back to the previous setting page.
- Click **Reset** to reset settings on this page.
- Click **Run** to execute the setups now.

Back Up Configuration

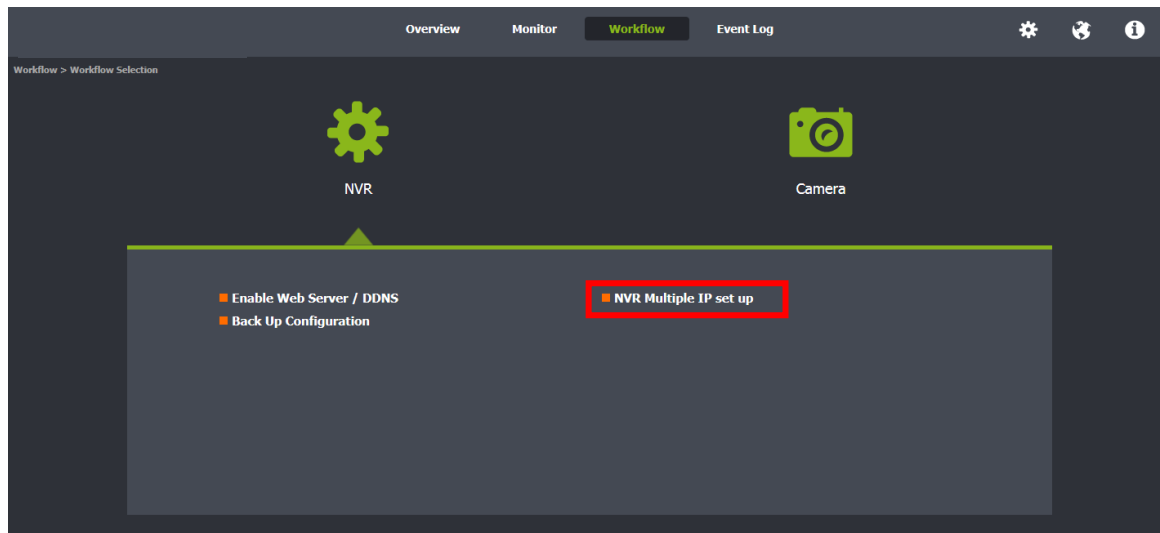


Follow the instruction flow on the right. The configurations can be saved as backup and restored when needed to save time and effort.

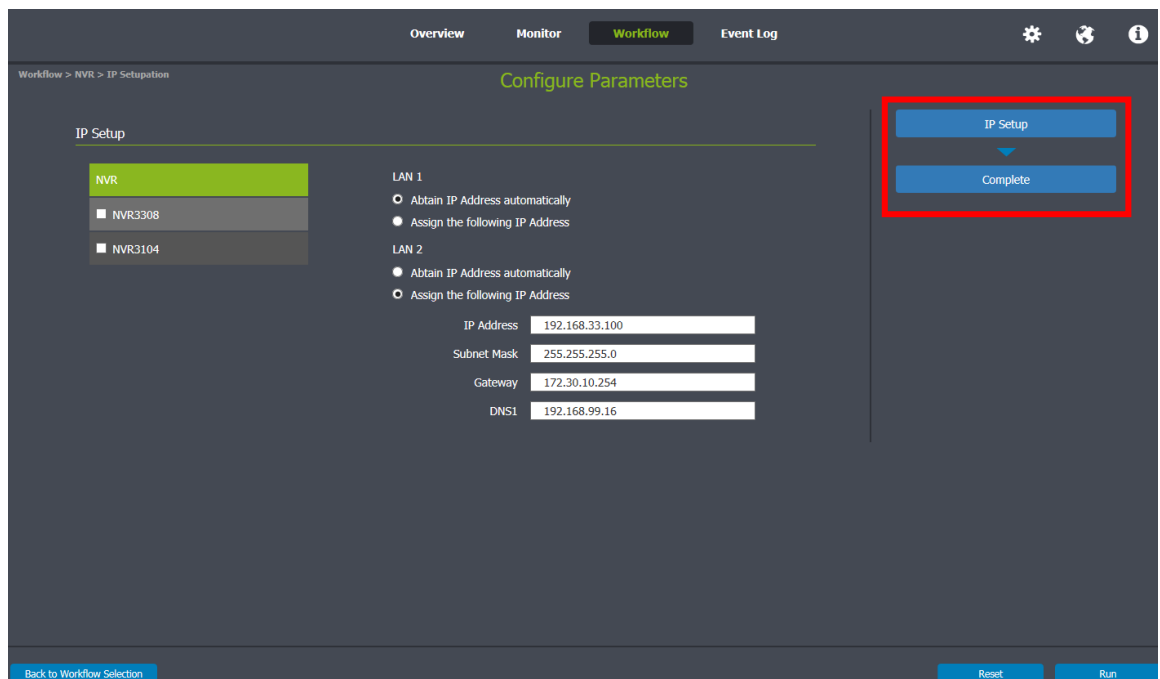


1. Select **Backup** or **Restore**.
2. Select path to save the configurations.
3. Select which device you'd like to save its configurations.
 - Click **Back to Workflow Selection** to go back to the previous setting page.
 - Click **Reset** to reset settings on this page.
 - Click **Run** to execute the setups now.

NVR Multiple IP Setup



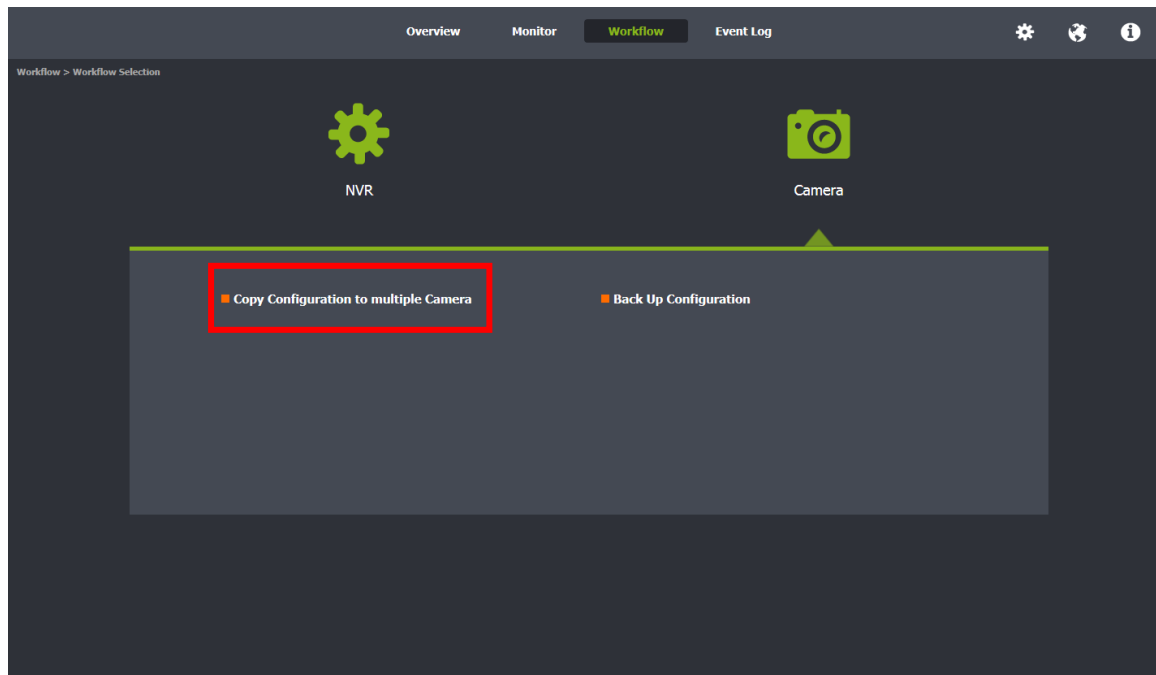
Follow the instruction flow on the right. Multiple IP addresses are supported. You can select the Obtain IP Address Automatically or Assign the following IP Address and input detailed information for each NVR.



- Click **Back to Workflow Selection** to go back to the previous setting page.
- Click **Reset** to reset settings on this page.
- Click **Run** to execute the setups now.

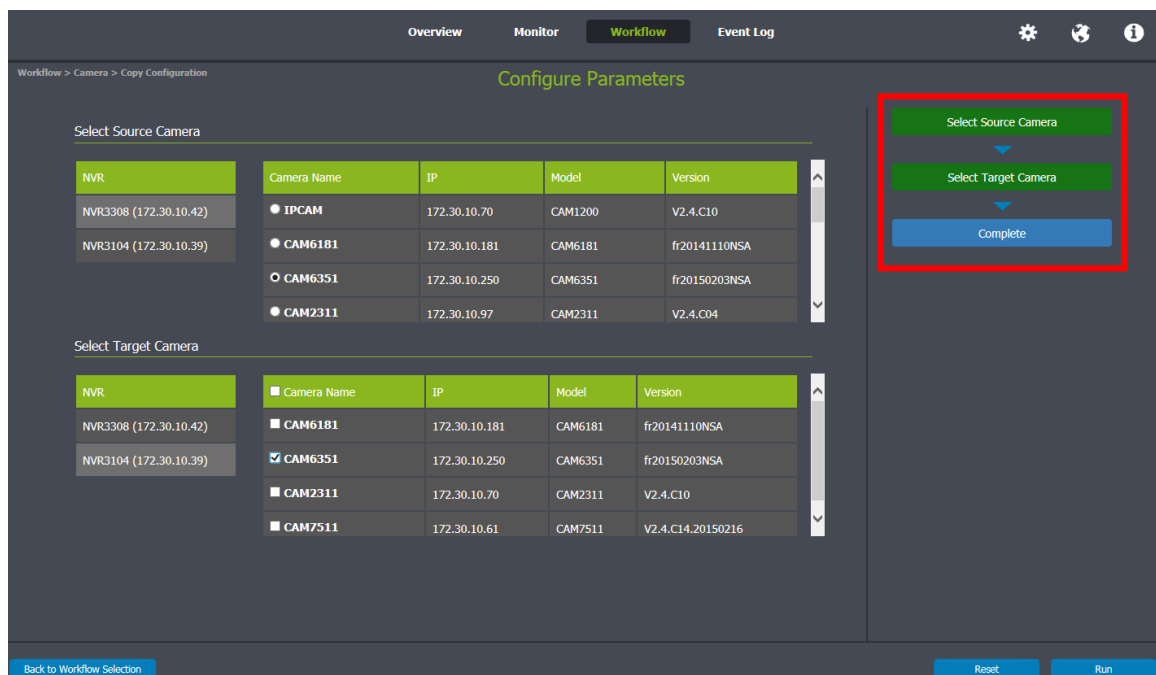
13.5.2. Camera

Copy Configuration to Multiple Cameras



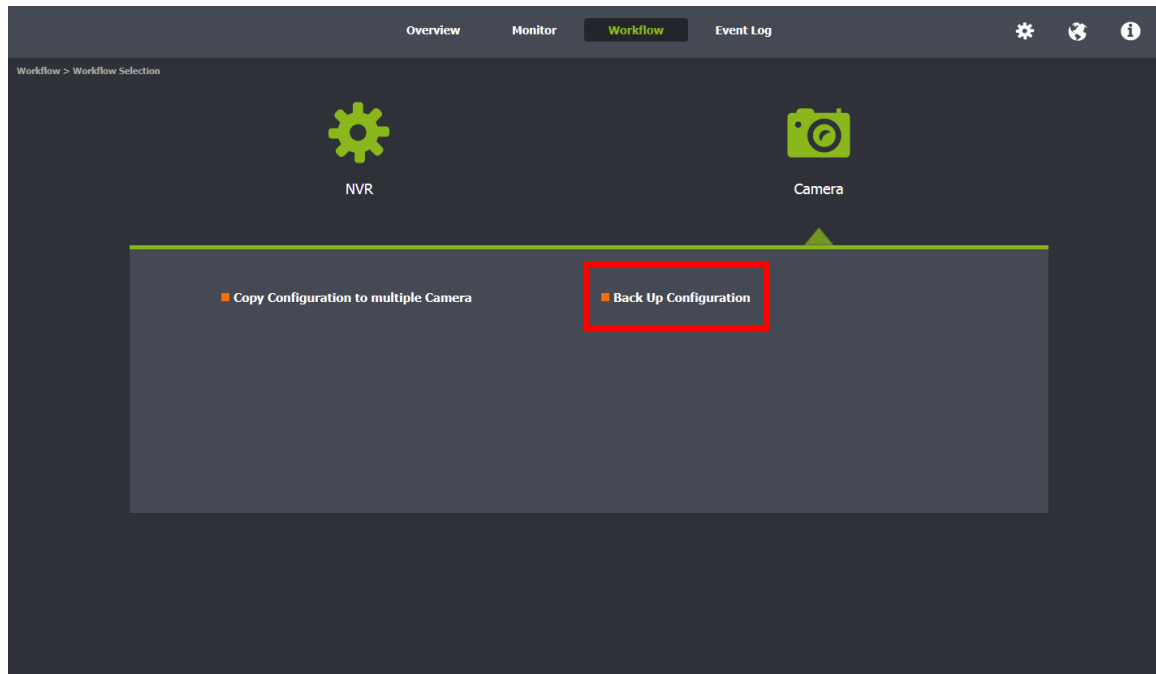
Follow the instruction flow on the right. The configurations can be saved as backup and restored when needed to save time and effort.

Note: The source camera and the target camera should bear the same model and version.

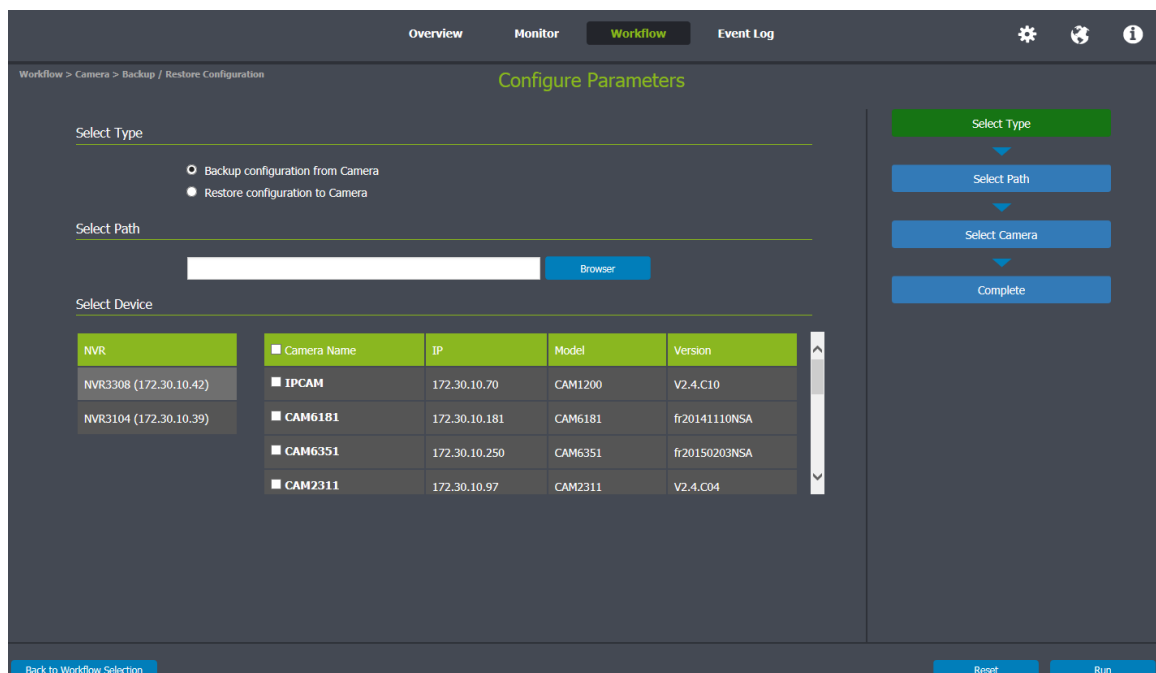


1. Select the source NVR and the cameras under this NVR.
 2. Select the target NVR and the cameras under this NVR.
- Click **Back to Workflow Selection** to go back to the previous setting page.
 - Click **Reset** to reset settings on this page.
 - Click **Run** to execute the setups now.

Backup Configuration



Follow the instruction flow on the right. The configurations can be saved as backup and restored when needed to save time and effort.



1. Select **Backup** or **Restore**.
2. Select path to save the configurations.
3. Select which device you'd like to save its configurations.
 - Click **Back to Workflow Selection** to go back to the previous setting page.
 - Click **Reset** to reset settings on this page.
 - Click **Run** to execute the setups now.

13.6. Event Log

See the detailed event status with information such as source, severity, date/Time and Event here. With classified event logs, users can identify which event needs to take actions first and which not to respond to the situations more quickly and efficiently.

Overview Monitor Workflow Event Log				
All	search	Export	1 2 3 ... 11	
NVR	SOURCE	Severity	Date / Time	Event
NVR3308 (172.30.10.42)	IPCAM	✓	2015-06-30 14:44:27	admin 127.0.0.1 login success
NVR3104 (172.30.10.39)	NVR3308 (172.30.10.42)	✓	2015-06-30 14:46:08	NVR service start
	CAM1301	⚡	2015-06-30 14:46:18	Video Loss Happened[5]
	ONVIF	⚡	2015-06-30 14:46:18	Video Loss Happened[11]
	ONVIF	⚡	2015-06-30 14:46:19	Video Loss Happened[12]
	CAM2311	✓	2015-06-30 14:46:34	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:37	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:40	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:43	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:46	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:49	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:52	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:55	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:46:57	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:47:00	VI(camera motion) happened
	CAM2311	✓	2015-06-30 14:47:04	VI(camera motion) happened

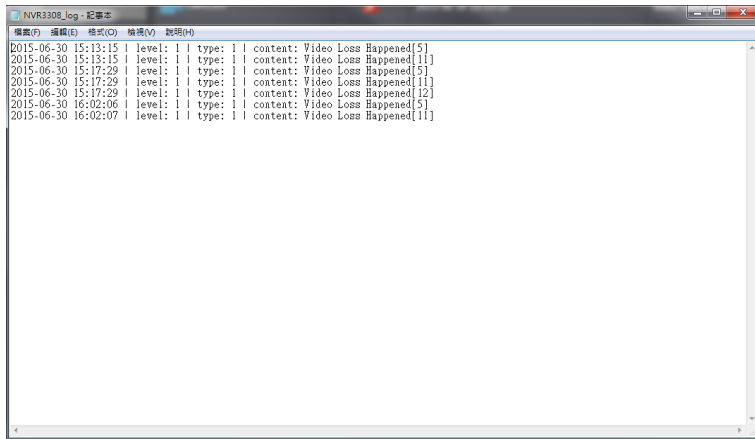
Search

Use the drop-down list to filter the specific event, such as All, Normal, Warning, Error, Critical Error, you'd like to search and click Search or Export.

All	search	Export	1 2 3 4 5 6 7 ... 11	
Normal				
Warning				
Error				
Critical Error				
NVR	SOURCE	Severity	Date / Time	Event
NVR3308 (172.30.10.42)	CAM6351	✓	2015-06-30 15:41:48	VI(camera motion) happened
NVR3104 (172.30.10.39)	CAM6351	✓	2015-06-30 15:41:51	VI(camera motion) happened
	CAM6351	✓	2015-06-30 15:41:55	VI(camera motion) happened
	CAM6351	✓	2015-06-30 15:41:57	VI(camera motion) happened
	CAM6351	✓	2015-06-30 15:42:00	VI(camera motion) happened

Export

Click Export, the log you're looking for will be copied to the notebook as shown below.



Click on the number on the upper right corner to jump to the corresponding page to see the log.

